

Ny dataskyddslag

Kompletterande bestämmelser
till EU:s dataskyddsförordning

Betänkande av Dataskyddsutredningen

Stockholm 2017

SOU och Ds kan köpas från Wolters Kluwers kundservice.
Beställningsadress: Wolters Kluwers kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@wolterskluwer.se
Webbplats: wolterskluwer.se/offentligapublikationer

För remissutsändningar av SOU och Ds svarar Wolters Kluwer Sverige AB
på uppdrag av Regeringskansliets förvaltningsavdelning.

Svara på remiss – hur och varför

Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).

En kort handledning för dem som ska svara på remiss.

Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remisser

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck: Elanders Sverige AB, Stockholm 2017

ISBN 978-91-38-24607-8

ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet

Regeringen beslutade den 25 februari 2016 att tillkalla en särskild utredare med uppdrag att föreslå de anpassningar och kompletterande författningsbestämmelser på generell nivå som den nya dataskyddsförordningen ger anledning till (dir. 2016:15).

Som särskild utredare förordnades samma dag justitierådet Inga-Lill Askersjö.

Som experter att biträda utredningen förordnades den 23 mars 2016 juristen Carolina Brånby, dataskyddschefen Caroline Olstedt Carlström, rättssakkunnige Manne Heimer, rättsliga utredaren Per Kjellsson, chefsjuristen Hans-Olof Lindblom, kammarrättsrådet Elisabet Reimers, doktoranden Daniel Westman samt förbundsjuristen Staffan Wikell. Elisabet Reimers entledigades från uppdraget den 15 december 2016.

Som sakkunnig i utredningen förordnades den 1 november 2016 chefsrådmannen Maria Eka, som även har haft ett särskilt uppdrag att bistå sekretariatet med vissa frågor.

Som sekreterare anställdes den 1 mars 2016 juristen Maria Jonsson och den 17 mars 2016 enhetschefen Ulrika Söderqvist. Den 15 oktober 2016 anställdes rättsliga specialisten Jenny Nyman för tiden till och med den 31 mars 2017.

Utredningen, som har tagit sig namnet Dataskyddsutredningen, överlämnar härmed betänkandet Ny dataskyddslag (SOU 2017:39). Experterna och den sakkunniga har deltagit i utredningsarbetet i sådan utsträckning att det har varit motiverat att formulera betänkandet i vi-form. Uppdraget är härmed slutfört.

Stockholm den 12 maj 2017

Inga-Lill Askersjö

*/ Ulrika Söderqvist
Maria Jonsson
Jenny Nyman*

Innehåll

Förkortningar	15
Sammanfattning	19
Summary	29
1 Författningsförslag	39
1.1 Förslag till lag med kompletterande bestämmelser till EU:s dataskyddsförordning.....	39
1.2 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400).....	51
1.3 Förslag till förordning om ändring i arkivförordningen (1991:446).....	53
1.4 Förslag till förordning med kompletterande bestämmelser till EU:s dataskyddsförordning.....	55
2 Vårt uppdrag och arbete	59
2.1 Uppdraget.....	59
2.2 Avgränsningar	59
2.3 Utredningsarbetet.....	60
3 Gällande rätt	63
3.1 Inledning.....	63
3.2 Internationella överenskommelser	64
3.2.1 Förenta Nationerna.....	64

3.2.2	OECD	64
3.3	Europarätt	65
3.3.1	Europarådet	65
3.3.2	Europeiska unionen	66
3.4	Svensk rätt	68
3.4.1	Regeringsformen	68
3.4.2	Dataskyddsdirektivets genomförande	68
4	EU:s dataskyddsreform	71
4.1	Allmänt om reformen	71
4.2	Dataskyddsförordningen	72
4.2.1	Förordningens syfte	73
4.2.2	Tillämpningsområdet	73
4.2.3	Sakliga förändringar	75
5	Ett nytt svenskt regelverk om dataskydd	77
5.1	Vårt uppdrag	77
5.2	Överväganden och förslag	78
5.2.1	Personuppgiftslagen, personuppgiftsförordningen och Datainspektionens föreskrifter ska upphävas	78
5.2.2	Ett regelverk som kompletterar dataskyddsförordningen på generell nivå ska införas	79
5.2.3	Avvikande bestämmelser i annan lag eller i förordning ska ha företräde	83
6	Behandling av personuppgifter utanför dataskyddsförordningens tillämpningsområde	87
6.1	Vårt uppdrag	87
6.2	Gällande rätt	87
6.3	Dataskyddsförordningen	88
6.4	Överväganden och förslag	89

6.4.1	Vad faller utanför unionsrättens tillämpningsområde?	90
6.4.2	Ska förordningens bestämmelser göras gällande utanför deras tillämpningsområde?	91
6.4.3	Vem ska utöva tillsyn?	93
7	Förhållandet till yttrande- och informationsfriheten	95
7.1	Vårt uppdrag.....	95
7.2	Gällande rätt.....	95
7.3	Dataskyddsförordningen.....	98
7.4	Våra överväganden och förslag.....	98
8	Rättslig grund för behandling av personuppgifter	103
8.1	Vårt uppdrag.....	103
8.2	Dataskyddsförordningen.....	103
8.2.1	Laglig behandling.....	103
8.2.2	Begreppet nödvändig.....	105
8.2.3	Förhållandet mellan artiklarna 5 och 6 i dataskyddsförordningen	106
8.3	Överväganden och förslag.....	108
8.3.1	Grunden för behandlingen ska i vissa fall vara fastställd	108
8.3.2	Behandling för att uppfylla en rättslig förpliktelse	113
8.3.3	Behandling som ett led i myndighetsutövning	119
8.3.4	Behandling för att utföra uppgifter av allmänt intresse	122
8.3.5	Särskilda bestämmelser som anpassar tillämpningen av dataskyddsförordningen.....	133
8.3.6	Inledande upplysningsbestämmelse	135
8.4	Sammanfattning	135

9	Barns samtycke som rättslig grund	137
9.1	Vårt uppdrag	137
9.2	Gällande rätt	137
9.3	Dataskyddsförordningen	138
9.3.1	Samtycke som rättslig grund för behandling av personuppgifter	138
9.3.2	Personuppgifter som rör barn förtjänar ett särskilt skydd.....	140
9.3.3	Barns samtycke.....	141
9.4	Utgångspunkter för vår bedömning.....	142
9.4.1	Inledning.....	142
9.4.2	Barnets bästa och barnets rätt till integritet	142
9.4.3	När är artikel 8.1 i dataskyddsförordningen tillämplig?	144
9.4.4	Något om olika åldersgränser i svensk lagstiftning.....	149
9.4.5	Direktreklam till barn	151
9.4.6	Yttranden till utredningen angående åldersgränsen	152
9.5	Överväganden och förslag.....	153
10	Känsliga personuppgifter	161
10.1	Vårt uppdrag	161
10.2	Dataskyddsförordningen	161
10.3	Vad betyder kravet på stöd i nationell rätt?	162
10.4	Den registrerades samtycke	166
10.4.1	Gällande rätt	166
10.4.2	Överväganden.....	166
10.5	Arbetsrätt, social trygghet och socialt skydd	167
10.5.1	Gällande rätt	167
10.5.2	Överväganden och förslag	167
10.6	Viktigt allmänt intresse	171
10.6.1	Gällande rätt	171

10.6.2	Överväganden och förslag.....	172
10.7	Hälso- och sjukvård och social omsorg.....	182
10.7.1	Gällande rätt	182
10.7.2	Överväganden och förslag.....	184
10.8	Folkhälsa.....	186
10.8.1	Gällande rätt	186
10.8.2	Överväganden	187
11	Personuppgifter som rör lagöverträdelser.....	189
11.1	Vårt uppdrag.....	189
11.2	Gällande rätt	189
11.3	Dataskyddsförordningen.....	191
11.4	Överväganden och förslag.....	192
12	Personnummer och samordningsnummer	197
12.1	Vårt uppdrag.....	197
12.2	Gällande rätt	197
12.3	Dataskyddsförordningen.....	198
12.4	Överväganden och förslag.....	199
13	Begränsningar av vissa rättigheter och skyldigheter i dataskyddsförordningen	201
13.1	Vårt uppdrag.....	201
13.2	Dataskyddsförordningen.....	201
13.3	Gällande rätt	203
13.4	Överväganden och förslag.....	204
13.4.1	Sekretess och tystnadsplikt ska gå före informationsplikten.....	204
13.4.2	Löpande text som utgör utkast eller minnesanteckning ska inte omfattas av rätten till registerutdrag	206
13.4.3	Något om rätten att göra invändningar	207

13.4.4	Regeringen ska få meddela föreskrifter om ytterligare undantag.....	208
14	Arkiv och statistik	209
14.1	Vårt uppdrag	209
14.2	Gällande rätt	210
14.3	Dataskyddsförordningen	211
14.3.1	Direkt tillämpliga bestämmelser	211
14.3.2	Bestämmelser som ger utrymme för nationella undantag	213
14.4	Överväganden och förslag – arkivändamål av allmänt intresse	214
14.4.1	Allmänt intresse	214
14.4.2	Rättslig grund och tillåten vidarebehandling.....	215
14.4.3	Förhållandet till arkivlagstiftningen och behandling av känsliga personuppgifter.....	220
14.4.4	Lämpliga skyddsåtgärder	223
14.4.5	Undantag från vissa av den registrerades rättigheter	228
14.4.6	Organ som bör jämföras med myndigheter	233
14.5	Överväganden och förslag – statistiska ändamål	234
14.5.1	Statistik	234
14.5.2	Rättslig grund och tillåten vidarebehandling.....	235
14.5.3	Känsliga personuppgifter	236
14.5.4	Lämpliga skyddsåtgärder	238
14.5.5	Undantag från vissa av den registrerades rättigheter	240
15	Förhandstillstånd	243
15.1	Vårt uppdrag	243
15.2	Gällande rätt	243
15.3	Dataskyddsförordningen	244
15.4	Överväganden	244

16	Godkännande av certifieringsorgan	247
16.1	Vårt uppdrag.....	247
16.2	Dataskyddsförordningen.....	247
16.3	Överväganden	249
16.3.1	Certifiering, ackreditering och Swedac	249
16.3.2	Vår bedömning	249
17	Sekretess.....	253
17.1	Vårt uppdrag.....	253
17.2	Allmänt om grundlags- och sekretessregleringen.....	253
17.3	Sekretess hos tillsynsmyndigheten	255
17.3.1	Gällande rätt	255
17.3.2	Dataskyddsförordningen	257
17.3.3	Överväganden	257
17.4	Tystnadsplikt för dataskyddsombud	259
17.4.1	Gällande rätt	259
17.4.2	Dataskyddsförordningen	259
17.4.3	Överväganden och förslag.....	260
17.5	Sekretess för uppgifter som behandlas i strid mot personuppgiftsregleringen.....	263
17.5.1	Gällande rätt	263
17.5.2	Överväganden och förslag.....	265
17.6	Generalklausulen.....	267
17.6.1	Gällande rätt	267
17.6.2	Överväganden och förslag.....	268
17.7	Sekretess för uppgifter i verksamhet för teknisk bearbetning och lagring	269
17.7.1	Gällande rätt	269
17.7.2	Överväganden och förslag.....	270
18	Sanktioner	273
18.1	Vårt uppdrag.....	273
18.2	Vad är en sanktion?	273

18.3	Gällande rätt	274
18.3.1	Skadestånd	274
18.3.2	Straff.....	275
18.3.3	Vite.....	276
18.4	Dataskyddsförordningen	277
18.4.1	Skadestånd	277
18.4.2	Administrativa sanktionsavgifter	278
18.4.3	Andra sanktioner.....	281
18.5	Sanktionsavgifter inom offentlig sektor	281
18.5.1	Vad är en sanktionsavgift?.....	281
18.5.2	Viten och sanktionsavgifter mot det allmänna....	282
18.5.3	Överväganden och förslag	287
18.6	Övriga sanktioner och förbudet mot dubbelbestraffning.....	291
18.6.1	Medlemsstaternas åligganden.....	291
18.6.2	Allmänt om kriminalisering	292
18.6.3	Dubbelprövningsförbudet.....	294
18.6.4	Överväganden och förslag	294
18.7	Betalning och verkställighet.....	298
18.7.1	Överväganden och förslag	298
19	Processuella frågor.....	299
19.1	Vårt uppdrag	299
19.2	Kapitlets disposition.....	300
19.3	Rättsmedel mot den personuppgiftsansvarige eller personuppgiftsbiträdet.....	300
19.3.1	Gällande rätt	300
19.3.2	Dataskyddsförordningen.....	301
19.3.3	Överväganden och förslag	302
19.4	Klagomål till tillsynsmyndigheten.....	305
19.4.1	Gällande rätt	305
19.4.2	Dataskyddsförordningen.....	305
19.4.3	Överväganden och förslag	305

19.5	En rättssäker handläggning hos tillsynsmyndigheten	308
19.5.1	Gällande rätt	308
19.5.2	Dataskyddsförordningen	309
19.5.3	Överväganden och förslag.....	310
19.6	Gemensamma tillsynsinsatser	319
19.6.1	Gällande rätt	319
19.6.2	Dataskyddsförordningen	321
19.6.3	Överväganden	323
19.7	Överklagande av tillsynsmyndighetens beslut	324
19.7.1	Gällande rätt	324
19.7.2	Dataskyddsförordningen	325
19.7.3	Överväganden och förslag.....	325
19.8	Överklagande av andra beslut	330
19.8.1	Överväganden och förslag.....	330
19.9	Ideella organisationer som är verksamma inom dataskyddsområdet	331
19.9.1	Dataskyddsförordningen	331
19.9.2	Överväganden	331
19.10	Parallella domstolsförfaranden.....	335
19.10.1	Dataskyddsförordningen	335
19.10.2	Överväganden	336
20	Ikraftträdande- och övergångsbestämmelser	339
20.1	Vårt uppdrag.....	339
20.2	Ikraftträdande- och övergångsbestämmelser i förordningen	339
20.3	Överväganden och förslag.....	340
21	Konsekvenser.....	345
21.1	Vårt uppdrag.....	345
21.2	Förändringar som följer av våra förslag.....	346

21.3	Ekonomiska konsekvenser.....	348
21.3.1	Ekonomiska konsekvenser för det allmänna.....	348
21.3.2	Ekonomiska konsekvenser för enskilda	349
21.4	Konsekvenser i övrigt.....	350
22	Författningskommentar	353
22.1	Förslaget till lag med kompletterande bestämmelser till EU:s dataskyddsförordning	353
22.2	Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)	387
Bilagor		
	Bilaga 1 Kommittédirektiv 2016:15	391
	Bilaga 2 Dataskyddsförordningen.....	417

Förkortningar

Artikel 29-gruppen	Artikel 29-arbetsgruppen för skydd av personuppgifter
dataskyddsdirektivet	Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter
dataskyddsförordningen	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)
dataskyddskonventionen	Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk data-behandling av personuppgifter
dataskyddsrambeslutet	Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete

DIFS	Datainspektionens författningssamling
dir.	direktiv
dnr	diarienummer
Ds	Departementsserien
EU	Europeiska unionen
EU-domstolen	Europeiska unionens domstol/ Europeiska gemenskapernas domstol
Europadomstolen	Europeiska domstolen för de mänskliga rättigheterna
Europakonventionen	Europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna
f.	följande sida/sidor
FN	Förenta Nationerna
förordning nr 45/2001	Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitu- tionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter
HFD	Högsta förvaltningsdomstolens årsbok
JK	Justitiekanslern
JO	Riksdagens ombudsmän
Ju	Justitiedepartementet
kommissionen	Europeiska kommissionen

LOU	lagen (2016:1145) om offentlig upphandling
NJA	Nytt juridiskt arkiv
nya dataskyddsdirektivet	Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF
OECD	Organisationen för ekonomiskt samarbete och utveckling
OSL	offentlighets- och sekretesslagen (2009:400)
prop.	regeringens proposition
PUF	personuppgiftsförordningen (1998:1191)
PUL	personuppgiftslagen (1998:204)
rskr.	riksdagsskrivelse
RÅ	Regeringsrättens årsbok
SOU	Statens offentliga utredningar

Sammanfattning

Inledning

EU:s nya dataskyddsförordning ska tillämpas från och med den 25 maj 2018. Dataskyddsförordningen är direkt tillämplig i Sverige men ger utrymme för kompletterande nationella bestämmelser av olika slag.

Vårt övergripande uppdrag har varit att föreslå en ny nationell reglering som på ett generellt plan kompletterar dataskyddsförordningen. I vårt uppdrag har däremot inte ingått att se över de s.k. registerförfattningarna eller annan sektorsspecifik reglering om behandling av personuppgifter. Vi har inte heller haft i uppdrag att analysera eller beskriva vilka förändringar som dataskyddsförordningen i sig innebär. Det är därmed bara ett fåtal av alla de frågor som regleras i dataskyddsförordningen som behandlas eller ens nämns i detta betänkande.

Vi har, inom ramen för vårt uppdrag, strävat efter att den personuppgiftsbehandling som är tillåten i dag i möjligaste mån ska kunna fortsätta. Vårt arbete har alltså inte syftat till att vare sig utvidga eller inskränka möjligheterna till behandling av personuppgifter, annat än då dataskyddsförordningen kräver en sådan förändring.

Ett nytt svenskt regelverk om dataskydd

Vi föreslår att personuppgiftslagen (1998:204) och personuppgiftsförordningen (1998:1191) ska upphävas och att de kompletterande bestämmelser som är av generell karaktär samlas i en ny övergripande lag och förordning om dataskydd. För att betona att författningarna inte är heltäckande, utan endast utgör komplement till dataskyddsförordningen, bör de benämnas lagen med kompletterande bestämmelser till EU:s dataskyddsförordning respektive förordningen med

kompletterande bestämmelser till EU:s dataskyddsförordning. Vi har valt att kalla den nya lagen *dataskyddslagen* i detta betänkande.

Dataskyddsförordningen ska gälla även i verksamhet som inte omfattas av unionsrätten

Behandling av personuppgifter som utförs som ett led i en verksamhet som inte omfattas av unionsrätten, t.ex. i verksamhet som rör nationell säkerhet, omfattas inte av dataskyddsförordningen. Detsamma gäller behandling av personuppgifter i verksamhet som omfattas av EU:s gemensamma utrikes- och säkerhetspolitik. För att säkerställa att det inom varje verksamhet finns ett fullgott skydd av personuppgifter anser vi dock att förordningens bestämmelser i tillämpliga delar bör gälla även i dessa fall. Vårt förslag om utsträckt tillämpningsområde hindrar dock inte att det för en viss sådan verksamhet införs en särskild reglering, om det skulle anses mer lämpligt.

Sektorsspecifika bestämmelser ska ha företräde framför dataskyddslagen

De bestämmelser som vi föreslår är av generell karaktär. På vissa områden kommer det att finnas behov av lag- eller förordningsbestämmelser kring behandling av personuppgifter som avviker från dataskyddslagens reglering. Det kan t.ex. röra sig om bestämmelser som specificerar den rättsliga grunden för en myndighets behandling av personuppgifter, begränsningar av rätten att behandla känsliga personuppgifter i en viss verksamhet eller särskilda förfaranderegler. Vi föreslår att sådana avvikande bestämmelser ska ha företräde framför dataskyddslagen. Det innebär dock inte att de därigenom också får företräde framför dataskyddsförordningen inom det aktuella området. För att en avvikande bestämmelse i exempelvis en registerförfattning ska kunna tillämpas, måste den vara förenlig med dataskyddsförordningen och avse en fråga som får särregleras genom nationell rätt.

Annorlunda förhåller det sig när det gäller verksamhet som inte omfattas av unionsrätten, dvs. där dataskyddsförordningen inte är direkt tillämplig men där den har fått ett utsträckt tillämpningsområde genom dataskyddslagen. I det fallet kan det genom ett undantag i lag eller förordning föreskrivas att dataskyddsförord-

ningen inte ska gälla i verksamheten. Ett sådant undantag kan också ange att endast vissa delar av dataskyddsförordningen inte ska gälla.

Förhållandet till våra grundlagar förändras inte

Våra detaljerade tryck- och yttrandefrihetsgrundlagar är unika i jämförelse med hur motsvarande reglering ser ut i övriga Europa. Data-skyddsförordningen inskränker inte möjligheterna att behandla personuppgifter på det grundlagsreglerade området. Det får inte råda någon osäkerhet kring detta, eftersom det skulle kunna få påverkan på vitala och mycket känsliga delar av den opinionsskapande verksamheten, såsom meddelarfrihet och källskydd. Vi föreslår därför en upplysningsbestämmelse som tydliggör att bestämmelserna i data-skyddsförordningen och i dataskyddslagen inte ska tillämpas i den utsträckning det skulle strida mot grundlagsbestämmelserna om tryck- och yttrandefrihet.

Utänför det grundlagsskyddade området föreslår vi att ett undantag från dataskyddsförordningen införs för sådan behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande. Vissa av dataskyddsförordningens bestämmelser, bland annat de som rör säkerhet för personuppgifter, ska dock tillämpas även i dessa fall.

Utrymmet för att ge offentlighetsprincipen företräde framför personuppgiftsregleringen är tydligt i dataskyddsförordningen. Tryckfrihetsförordningens reglering om allmänhetens tillgång till handlingar kan alltså fortsätta att tillämpas, även när det gäller allmänna handlingar som innehåller personuppgifter.

Barn som har fyllt 13 år ska i vissa fall kunna samtycka till behandling av personuppgifter

Enligt förordningen ska ett barn ha fyllt 16 år för att självt kunna samtycka till behandling av personuppgifter vid erbjudandet av informationssamhällets tjänster, t.ex. sociala medier, söktjänster och s.k. appar för smarta enheter. Vi föreslår att denna åldersgräns ska sänkas till 13 år i Sverige. För barn yngre än så krävs att samtycket lämnas av vårdnadshavaren eller att barnets samtycke godkänns av denne.

Rättsliga förpliktelser, myndighetsutövning och uppgifter av allmänt intresse ska vara särskilt reglerade för att utgöra rättslig grund

Enligt dataskyddsförordningen måste en rättslig förpliktelse, myndighetsutövning eller uppgift av allmänt intresse vara fastställd i enlighet med nationell rätt eller unionsrätt för att kunna utgöra rättslig grund för behandling av personuppgifter. Vi föreslår bestämmelser i dataskyddslagen som förtydligar hur dessa företeelser fastställs i enlighet med svensk rätt. En rättslig förpliktelse är enligt svensk rätt fastställd om den gäller enligt lag eller annan författning eller följer av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Myndighetsutövning fastställs i svensk rätt genom lag eller annan författning. Uppgifter av allmänt intresse är fastställda i enlighet med svensk rätt om de följer av lag eller annan författning eller av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning.

Med anledning av att vårt uppdrag har omfattat arkivfrågor har vi uppmärksammat att enskilda arkivinstitutioner kan sakna en fastställd rättslig grund för behandling av personuppgifter. I avvaktan på den breda översyn av arkivväsendet som regeringen har aviserat, föreslår vi att rättslig grund ska kunna fastställas av Riksarkivet, genom föreskrifter eller beslut i enskilda fall.

Känsliga personuppgifter får behandlas bara om det uttryckligen är tillåtet

Enligt dataskyddsförordningen gäller som huvudregel, liksom tidigare, ett förbud mot behandling av känsliga personuppgifter. Behandling av sådana personuppgifter får ske bara om det finns stöd i någon av förordningens undantagsbestämmelser. Vissa undantag från förbudet följer direkt av förordningen, medan andra förutsätter stöd även i nationell rätt. Vi föreslår att ett sådant stöd ska införas i dataskyddslagen när det gäller nödvändig behandling av personuppgifter på arbetsrättens område, inom hälso- och sjukvård, i social omsorg, i arkivverksamhet och i statistisk verksamhet. Stödet för behandlingen ska vara förenat med vissa restriktioner.

Myndigheter ska få behandla känsliga personuppgifter med stöd av ett nytt myndighetsundantag

Myndigheter har ofta berättigade skäl att behandla känsliga personuppgifter och i många fall sker detta i den registrerades eget intresse. För att säkerställa att nödvändig behandling kan ske även efter det att dataskyddsförordningen börjar gälla bedömer vi att det krävs ett nytt undantag för behandling av känsliga personuppgifter hos myndigheter. Vi föreslår att sådan behandling ska få ske

- i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av ett ärende,
- om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag, eller
- i enstaka fall, om det är absolut nödvändigt för ändamålet med behandlingen och behandlingen inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

Vi föreslår också att det vid behandling som sker med stöd av det nya myndighetsundantaget ska vara förbjudet att använda sökbegrepp som avslöjar känsliga personuppgifter.

Personuppgifter som rör lagöverträdelser ska få behandlas av myndigheter och annars bara om det uttryckligen är tillåtet

Vi föreslår att behandling av personuppgifter som rör fällande domar i brottmål, lagöverträdelser som innefattar brott eller straffprocessuella tvångsmedel även fortsättningsvis ska få utföras av myndigheter.

För att andra än myndigheter ska få behandla sådana uppgifter föreslår vi att det måste finnas uttryckligt stöd i lag eller förordning eller i föreskrifter eller förvaltningsbeslut från Datainspektionen. Vi föreslår ett sådant stöd i lag när det gäller uppgifter som behandlas för arkivändamål av allmänt intresse, förutsatt att behandlingen sker som en följd av de skyldigheter att bevara och vårda handlingar som anges i arkivlagstiftningen och andra föreskrifter.

Personnummer får under vissa förutsättningar behandlas även i fortsättningen

Vi föreslår att uppgifter om personnummer eller samordningsnummer även fortsättningsvis ska få behandlas när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Det finns begränsningar för när arkiverade uppgifter och statistikuppgifter får användas för åtgärder mot den registrerade

Personuppgifter som behandlas enbart för arkivändamål av allmänt intresse eller för statistiska ändamål får enligt vårt förslag inte användas för att vidta åtgärder i fråga om den registrerade, annat än om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen.

Begränsningen i fråga om arkiverade uppgifter ska inte gälla för myndigheter. Det ska däremot begränsningen rörande statistikuppgifter göra.

Rätten till registerutdrag och information m.m. ska i vissa fall vara begränsad

Den registrerades rättigheter stärks genom dataskyddsförordningen. Dessa rättigheter är dock inte ovillkorliga. Vissa viktiga undantag från rättigheterna regleras direkt i förordningen. Vi föreslår därutöver att rätten till information och s.k. registerutdrag inte ska gälla uppgifter som omfattas av sekretess. Rätten till registerutdrag ska som huvudregel inte heller gälla personuppgifter som finns i löpande text som utgör utkast eller minnesanteckning. Hos Riksarkivet och andra arkivmyndigheter ska rätten till registerutdrag, rättelse m.m. vara begränsad när det gäller personuppgifter som finns i arkivmaterial som tagits emot för förvaring av myndigheten.

Vissa beslut som fattas av en personuppgiftsansvarig myndighet får överklagas till domstol

I likhet med vad som gäller enligt personuppgiftslagen ska vissa beslut som en myndighet fattar i egenskap av personuppgiftsansvarig kunna överklagas till allmän förvaltningsdomstol. Det gäller sådana beslut som myndigheten fattar med anledning av att den registrerade utövar sina rättigheter enligt dataskyddsförordningen. Det kan t.ex. röra sig om avslagsbeslut på begäran om att den registrerade ska få tillgång till sina personuppgifter, att uppgifter ska rättas eller raderas eller att en behandling ska begränsas.

Den registrerade kan begära skadestånd

Den registrerade har enligt dataskyddsförordningen rätt till ersättning från den personuppgiftsansvarige eller ett personuppgiftsbiträde om skada har uppstått på grund av överträdelser av förordningen. Vi föreslår att det i dataskyddslagen förtydligas att denna rätt till skadestånd även gäller vid överträdelser av bestämmelser i dataskyddslagen och andra författningar som kompletterar förordningen.

Datainspektionen ska utöva tillsyn

Datainspektionen ska vara den myndighet som ska utöva tillsyn och övervaka att bestämmelserna i dataskyddsförordningen och dataskyddslagen efterlevs. Inspektionens tillsynsbefogenheter anges i dataskyddsförordningen. Dessa befogenheter ska enligt vårt förslag gälla även vid tillsynen över att dataskyddslagen och annan kompletterande lagstiftning följs.

Datainspektionens beslut enligt dataskyddsförordningen och dataskyddslagen får överklagas till allmän förvaltningsdomstol.

Datainspektionen ska behandla klagomål inom tre månader

Om en registrerad anser att personuppgifter behandlas på ett sätt som strider mot dataskyddsförordningen kan ett klagomål lämnas in till Datainspektionen. Klagomålet ska behandlas inom tre månader. Om det inte sker får den registrerade enligt vårt förslag begära ett

besked i frågan om Datainspektionen avser att utöva tillsyn eller inte. Om Datainspektionen behöver mer tid för att behandla klagomålet, får begäran avslås genom ett motiverat beslut. Den registrerade får överklaga detta beslut till allmän förvaltningsdomstol genom en s.k. dröjsmålstalan.

Sanktionsavgift kan tas ut även av myndigheter som gör fel

Genom dataskyddsförordningen införs en möjlighet för Datainspektionen att ta ut en administrativ sanktionsavgift av ett företag eller andra enskilda som bryter mot dataskyddsregleringen. En sådan sanktionsavgift ska enligt vårt förslag även kunna tas ut av en myndighet.

Vi föreslår inte någon straffbestämmelse motsvarande den som gäller enligt personuppgiftslagen.

Sekretessfrågor

Genom dataskyddsförordningen införs en skyldighet för myndigheter och vissa företag att utse ett dataskyddsbud. Ombudet ska vara bundet av sekretess enligt unionsrätten eller den nationella rätten.

För dataskyddsbud som deltar i det allmännas verksamhet gäller offentlighets- och sekretesslagens bestämmelser om sekretess. För den privata sektorn föreslår vi att tystnadsplikt ska gälla för dataskyddsbud i fråga om sådant som ombudet har fått veta om enskilds personliga eller ekonomiska förhållanden.

Konsekvenser

Dataskyddsförordningens direkt tillämpliga bestämmelser kommer att leda till konsekvenser, både för det allmänna och för enskilda. Vi har dock inte haft i uppgift att bedöma eller redovisa dessa konsekvenser. I vårt uppdrag ingår däremot att bedöma konsekvenserna av våra förslag, i den mån dessa medför förändringar jämfört med vad som gäller i dag.

Våra förslag innebär att Riksarkivet, Datainspektionen och de allmänna förvaltningsdomstolarna får något fler arbetsuppgifter. Vi

bedömer dock att kostnadsökningarna för berörda aktörer inte kommer att bli större än att de ryms inom de befintliga anslagen.

Våra förslag medför inga nya kostnader eller ökad administrativ börda för enskilda.

Vi anser att förslagen stärker skyddet för enskildas personliga integritet.

Summary

Introduction

The EU's new General Data Protection Regulation begins to apply on 25 May 2018. The General Data Protection Regulation will be directly applicable in Sweden, but it provides scope for supplementary national provisions of various kinds.

Our overarching remit was to propose a new national regulation that supplements the General Data Protection Regulation at a general level. However, our remit did not include reviewing the 'register statutes' or other sector-specific regulations on the processing of personal data. Nor did our remit include analysing or describing any changes that the General Data Protection Regulation in itself entails. Therefore, only a few of all the issues regulated in the General Data Protection Regulation are dealt with or even mentioned in this report.

Within the framework of our remit, we have endeavoured to ensure that the personal data processing currently permitted is able to continue as far as possible. Our work was therefore not intended to broaden or restrict the possibilities of processing personal data, other than in cases where the General Data Protection Regulation requires such a change.

A new Swedish regulatory framework on data protection

We propose that the Personal Data Act (1998:204) and the Personal Data Ordinance (1998:1191) should be repealed and that the supplementary provisions of a general nature should be collected in a new overall act and ordinance on data protection. To emphasise the fact that the statutes are not comprehensive and that they are simply a supplement to the General Data Protection Regulation, they should

be named the Act containing supplementary provisions to the EU General Data Protection Regulation and the Ordinance containing supplementary provisions to the EU General Data Protection Regulation. In this report, we have chosen to refer to the new act as the *Data Protection Act*.

The General Data Protection Regulation also to apply to activities not covered by EU law

The processing of personal data carried out as part of an activity not covered by EU law, e.g. activities concerning national security, is not covered by the General Data Protection Regulation. The same applies to the processing of personal data in activities covered by the EU Common Foreign and Security Policy. However, to ensure that there is sufficient protection of personal data in each activity, we consider that the relevant parts of the Regulation's provisions should apply in these cases as well. Yet our proposal on expanding the field of application would not preclude the introduction of a separate regulation for a certain activity of this kind, if deemed more appropriate.

Sector-specific provisions to take precedence over the Data Protection Act

The provisions we propose are of a general nature. In certain areas, there will be a need for provisions in acts or ordinances concerning processing of personal data that deviate from the regulations in the Data Protection Act. That may include provisions specifying the legal basis for a public authority's processing of personal data, restrictions on the right to process sensitive personal data in a certain activity or special procedural rules. We propose that such deviating provisions should take precedence over the Data Protection Act. However, this does not mean that they would thus also take precedence over the General Data Protection Regulation within the area in question. In order for a deviating provision in, for example, a register statute to be applied, it has to be compatible with the General Data Protection Regulation and refer to an issue that is allowed to be subject to special rules in national law.

The situation is different with regard to activities that are not covered by EU law, i.e. when the General Data Protection Regulation is not directly applicable but it has been given a broader field of application through the Data Protection Act. In such cases, it may be prescribed through an exemption in an act or ordinance that the General Data Protection Regulation does not apply to that specific activity. Such an exemption may also state that only certain parts of the General Data Protection Regulation do not apply.

No changes in relation to our constitution

Our detailed Fundamental Law on Freedom of Expression and Freedom of the Press Act are unique compared with corresponding regulations in the rest of Europe. The General Data Protection Act does not limit the possibilities of processing personal data in the area governed by the constitution. There must be no uncertainty about this, since such uncertainty could have an impact on vital and very sensitive parts of opinion-making activities, such as freedom of communication and protection of sources. We therefore propose an information provision to make clear that the provisions of the General Data Protection Regulation and the Data Protection Act must not be applied to the extent that they contravene the constitutional provisions on freedom of the press and freedom of expression.

Beyond the area protected by the constitution, we propose that an exemption from the General Data Protection Regulation be introduced for the processing of personal data that occurs for journalistic purposes or for academic, artistic or literary expression. However, some of the provisions in the General Data Protection Regulation, including those concerning the security of personal data, should be applied in these cases as well.

The scope for allowing the principle of public access to official documents to take priority over the personal data regulations is clear in the General Data Protection Regulation. This means that the rules contained in the Freedom of the Press Act on public access to documents can continue to be applied, also when it comes to official documents that contain personal data.

Children who are 13 and above in certain cases to be able to consent to the processing of their personal data

Under the General Data Protection Regulation, a child must be 16 to be able to give their own consent to the processing of personal data in relation to offers of information society services, such as social media, search engines and apps for smart devices. We propose that this age limit be lowered to 13 in Sweden. For younger children, consent must be given by a custodial parent or the child's consent must be approved by the custodial parent.

Legal obligations, exercise of official authority and tasks carried out in the public interest to be subject to separate regulations to form a legal basis

Under the General Data Protection Regulation, a legal obligation, the exercise of official authority or tasks carried out in the public interest must be laid down by national law or EU law to be able to form a legal basis for the processing of personal data. We propose provisions in the Data Protection Act that clarify how these phenomena are established in line with Swedish law. Under Swedish law, a legal obligation is established if it applies under an act or other statute or follows from collective agreements or decisions issued pursuant to an act or other statute. Exercise of official authority is established under Swedish law through an act or other statute. Under Swedish law, a task carried out in the public interest is established if it follows from an act or other statute or from collective agreements or decisions issued pursuant to an act or other statute.

Because our remit covered archive issues, we have drawn attention to the fact that private archive institutions might lack an established legal basis for processing personal data. Pending the broad review of the archive system that the Government has announced, we propose that it should be possible for the National Archives to establish a legal basis through regulations or decisions in individual cases.

Sensitive personal data may be processed only if explicitly permitted

Under the General Data Protection Regulation, the general rule, as before, is that processing of sensitive personal data is prohibited. Processing of such personal data may only be carried out if there is support for this in one of the Regulation's exemption clauses. Certain exemptions from the general rule follow directly from the Regulation, whereas others require support in national law as well. We propose that this kind of support be introduced in the Data Protection Act with regard to necessary processing of personal data in the area of employment law, health and medical care, social care, archive activities and statistics activities. Support for processing must be linked to certain restrictions.

Authorities to be able to process sensitive personal data under a new authority exception

Authorities often have legitimate reasons for processing sensitive personal data, and in many cases this is done in the data subject's own interests. To ensure that the necessary processing can be carried out even after the General Data Protection Regulation begins to apply, we consider that there is a need for a new exception regarding the processing of sensitive personal data held by authorities. We propose that such processing may be carried out:

- in running text if the data was provided in a matter or is required to deal with a matter;
- if the data was provided to the authority and processing is required by law; or
- in individual cases, if it is absolutely necessary for the purpose of the processing and the processing does not entail an improper intrusion on the personal privacy of the data subject.

We further propose that when carrying out processing under the new authority exception, using search terms that reveal sensitive personal data it is to be prohibited.

Personal data that concerns criminal offences to be processed by authorities and otherwise only if explicitly permitted

We propose that authorities should continue to be able to process personal data that concerns criminal convictions and offences or coercive measures under criminal law.

For actors other than authorities to be able to process such data, we propose that there must be explicit support in an act or ordinance or in regulations or administrative orders issued by the Swedish Data Protection Authority. We propose that support of this kind be laid down in law with regard to data processed for archiving purposes in the public interest, provided that the processing is carried out as a result of the obligations to protect and preserve documents specified in archive legislation and other provisions.

Under certain circumstances, personal identity numbers to continue to be processed

We propose that data concerning personal identity numbers or coordination numbers may continue to be processed when clearly justified with respect to the purpose of the processing, the importance of positive identification or some other significant reason.

There are restrictions on when archived data and statistics may be used for measures against a data subject

Under our proposal, personal data processed exclusively for archiving purposes in the public interest or for statistical purposes may not be used to take action in matters concerning the data subject unless there are exceptional grounds for doing so with respect to the person's vital interests.

Regarding archived data, this restriction will not apply to authorities. However, the restriction regarding statistical data will apply to authorities.

In some cases, the right to access to the personal data and information, etc. to be restricted

The rights of data subjects are strengthened under the General Data Protection Regulation. However, these rights are not unconditional. Certain important exceptions from the rights are regulated directly in the Regulation. In addition, we propose that the right to information and access to the personal data should not apply to data that is subject to secrecy regulations. As a general rule, the right to access to the personal data should not apply to personal data contained in running texts that constitute rough drafts or notes. Furthermore, the right to access to the personal data, rectification, etc. is to be restricted as regards personal data contained in archive material received for storage by the National Archives and other archiving authorities.

Certain decisions taken by an authority acting as controller of personal data may be appealed to a court of law

As is the case with the provisions of the Personal Data Act, it will be possible to appeal certain decisions taken by an authority in its capacity as controller of personal data to an administrative court. This applies to decisions taken by the authority in response to data subjects exercising their rights under the General Data Protection Regulation. For example, this may concern the rejection of a request by a data subject to obtain access to the personal data, that data be rectified or erased, or that the processing be restricted.

The data subject may seek compensation

Under the General Data Protection Regulation, the data subject is entitled to compensation from the controller or processor for damage suffered as a result of an infringement of the Regulation. We propose that the Data Protection Act should clarify that this right to compensation also applies to infringements of the Data Protection Act and other legislation that supplements the Regulation.

Swedish Data Protection Authority to exercise supervision

The Swedish Data Protection Authority will be the authority tasked with supervising and monitoring compliance with the provisions of the General Data Protection Regulation and the Data Protection Act. The Authority's supervisory powers are specified in the General Data Protection Regulation. Under our proposal, these powers should also apply to supervising compliance with the Data Protection Act and other supplementary legislation.

A decision taken by the Swedish Data Protection Authority under the General Data Protection Regulation and the Data Protection Act may be appealed to an administrative court.

Swedish Data Protection Authority to consider complaints within three months

Should a data subject consider that personal data is processed in a manner that contravenes the General Data Protection Regulation, they may lodge a complaint with the Swedish Data Protection Authority. Complaints are to be considered within three months. If this does not happen, under our proposal the data subject may request an indication as to whether or not the Swedish Data Protection Authority intends to exercise supervision. If the Swedish Data Protection Authority needs more time to consider the complaint, the request may be rejected through a reasoned decision. The data subject may appeal this decision to an administrative court by submitting a claim of delay.

Administrative fines may also be imposed on authorities that make errors

The General Data Protection Regulation provides the Swedish Data Protection Authority with the option of imposing administrative fines on an enterprise or other private party that violates data protection regulations. Under our proposal, it will also be possible to impose administrative fines on an authority that violates the General Data Protection Regulation.

We do not propose a penalty provision similar to that under the Personal Data Act.

Confidentiality issues

The General Data Protection Regulation introduces an obligation on authorities and certain other bodies to designate a data protection officer. This officer is to be bound by secrecy or confidentiality under EU law or national law.

Data protection officers who participate in public authority activities must abide by the confidentiality provisions of the Public Access to Information and Secrecy Act. Regarding the private sector, we propose that confidentiality should apply to data protection officers where the officer has gained knowledge of a private party's personal or financial circumstances.

Consequences

The directly applicable provisions of the General Data Protection Regulation will have consequences for both public institutions and private parties. However, it was not our task to assess or report on these consequences. Nonetheless, our remit does include assessing the consequences of our proposals insofar as they entail changes compared with what currently applies.

Our proposals entail a few more duties being assigned to the National Archives, the Swedish Data Protection Authority and the administrative courts. Our assessment, however, is that the increased costs to relevant actors will not exceed the scope of their existing appropriations.

Our proposals do not entail any new costs or increased administrative burden to private parties.

In our view, the proposals strengthen protection for the personal privacy of individuals.

1 Författningsförslag

1.1 Förslag till lag med kompletterande bestämmelser till EU:s dataskyddsförordning

Härigenom föreskrivs följande.

1 kap. Inledande bestämmelser

1 § Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), nedan kallad dataskyddsförordningen.

Termer och uttryck som används i denna lag har samma betydelse som i dataskyddsförordningen.

2 § Bestämmelserna i dataskyddsförordningen, i den ursprungliga lydelsen, och i denna lag ska i tillämpliga delar gälla även vid behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten och i verksamhet som omfattas av avdelning V kapitel 2 i fördraget om Europeiska unionen.

Avvikande bestämmelser i annan författning

3 § Om en annan lag eller en förordning innehåller någon bestämmelse som rör behandling av personuppgifter och som avviker från denna lag tillämpas den bestämmelsen.

Förhållandet till tryck- och yttrandefriheten

4 § Bestämmelserna i dataskyddsförordningen och i denna lag ska inte tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Bestämmelserna i kapitel II och III, artiklarna 24–30 och 35–43 och kapitel V i dataskyddsförordningen samt i 2–5 kap. denna lag ska inte tillämpas på behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

Organ som ska jämsställas med myndigheter

5 § Vid tillämpningen av 3 kap. 3 § 2 och 4 § samt 4 kap. 1 § andra stycket ska andra organ än myndigheter jämsställas med myndigheter, i den utsträckning bestämmelserna om allmänna handlingar och sekretess i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400) gäller i organets verksamhet.

Tystnadsplikt för dataskyddsombud

6 § Den som utsetts till dataskyddsombud enligt artikel 37 i dataskyddsförordningen får inte obehörigen röja det som han eller hon vid fullgörandet av sin uppgift har fått veta om enskilda personliga och ekonomiska förhållanden.

I det allmänna verksamheten tillämpas offentlighets- och sekretesslagen (2009:400) i stället för första stycket.

2 kap. Rättslig grund

1 § Av dataskyddsförordningen framgår att personuppgifter får behandlas endast om minst ett av de villkor som anges i artikel 6.1 i förordningen är uppfyllt.

2 § Vid erbjudande av informationssamhällets tjänster direkt till ett barn, ska vid tillämpningen av artikel 6.1 a i dataskyddsförordningen behandling av personuppgifter som rör ett barn vara tillåten om

barnet är minst 13 år. Om barnet är under 13 år ska sådan behandling vara tillåten endast om och i den mån samtycke ges eller godkänns av den person som har föräldraansvar för barnet.

Rättslig förpliktelse

3 § Personuppgifter får behandlas med stöd av artikel 6.1 c i data-skyddsförordningen om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som

1. gäller enligt lag eller annan författning,
2. följer av kollektivavtal, eller
3. följer av beslut som har meddelats med stöd av lag eller annan författning.

Uppgift av allmänt intresse och myndighetsutövning

4 § Personuppgifter får behandlas med stöd av artikel 6.1 e i data-skyddsförordningen om behandlingen är nödvändig

1. för att den personuppgiftsansvarige ska kunna utföra en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning, eller

2. som ett led i den personuppgiftsansvariges myndighetsutövning enligt lag eller annan författning.

Enskilda arkiv

5 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om behandling av personuppgifter för arkivändamål av allmänt intresse, när det gäller andra enskilda organ än de som omfattas av bestämmelserna om allmänna handlingar och sekretess i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400).

Den myndighet som regeringen bestämmer får även i enskilda fall besluta att sådana enskilda organ som avses i första stycket får behandla personuppgifter för arkivändamål av allmänt intresse.

3 kap. Vissa kategorier av personuppgifter

Känsliga personuppgifter

1 § Utöver vad som framgår av artikel 9.2 a, c, d, e eller f i dataskyddsförordningen får sådana särskilda kategorier av personuppgifter som anges i artikel 9.1 i dataskyddsförordningen (känsliga personuppgifter) behandlas om förutsättningarna i någon av 2–8 §§ är uppfyllda.

Arbetsrätt

2 § Känsliga personuppgifter får med stöd av artikel 9.2 b i dataskyddsförordningen behandlas om det är nödvändigt för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten.

Personuppgifter som behandlas med stöd av första stycket får lämnas ut till tredje part endast om det inom arbetsrätten finns en skyldighet att göra det eller om den registrerade uttryckligen har samtyckt till utlämnandet.

Myndigheters behandling i vissa fall

3 § Känsliga personuppgifter får med stöd av artikel 9.2 g i dataskyddsförordningen behandlas av en myndighet

1. i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av ett ärende,

2. om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag, eller

3. i enstaka fall, om det är absolut nödvändigt för ändamålet med behandlingen och behandlingen inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

4 § Vid behandling som sker enbart med stöd av 3 § får en myndighet inte använda sökbegrepp som avslöjar känsliga personuppgifter.

Hälso- och sjukvård och social omsorg

5 § Känsliga personuppgifter får med stöd av artikel 9.2 h i dataskyddsförordningen behandlas om behandlingen är nödvändig av skäl som hör samman med

1. förebyggande hälso- och sjukvård och yrkesmedicin,
2. bedömningen av en arbetstagares arbetskapacitet,
3. medicinska diagnoser,
4. tillhandahållande av hälso- och sjukvård eller behandling,
5. social omsorg, eller
6. förvaltning av social omsorg, hälso- och sjukvårdstjänster samt deras system.

Behandling enligt första stycket får ske under förutsättning att kravet på tystnadsplikt i artikel 9.3 i dataskyddsförordningen är uppfyllt.

Arkiv

6 § Känsliga personuppgifter får med stöd av artikel 9.2 j i dataskyddsförordningen behandlas för arkivändamål av allmänt intresse om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om bevarande och vård av arkiv.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att känsliga personuppgifter får behandlas för arkivändamål av allmänt intresse även i andra fall än de som avses i första stycket.

Den myndighet som regeringen bestämmer får även i enskilda fall besluta att andra enskilda organ än de som omfattas av bestämmelserna om allmänna handlingar och sekretess i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400) får behandla känsliga personuppgifter för arkivändamål av allmänt intresse.

Statistik

7 § Känsliga personuppgifter får med stöd av artikel 9.2 j i dataskyddsförordningen behandlas om behandlingen är nödvändig för statistiska ändamål och samhällsintresset av det statistikprojekt där

behandlingen ingår klart väger över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan innebära.

Bemyndigande

8 § Regeringen får meddela föreskrifter om ytterligare undantag från förbudet att behandla känsliga personuppgifter i artikel 9.1 i dataskyddsförordningen om det behövs med hänsyn till ett viktigt allmänt intresse.

Personuppgifter som rör lagöverträdelser

Behandling under kontroll av myndighet

9 § Personuppgifter som rör fällande domar i brottmål, lagöverträdelser som innefattar brott eller straffprocessuella tvångsmedel får enligt artikel 10 i dataskyddsförordningen behandlas av myndigheter.

10 § Den myndighet som regeringen bestämmer får i enskilda fall besluta att andra än myndigheter får behandla sådana uppgifter som avses i 9 §.

Arkiv

11 § Behandling av sådana personuppgifter som avses i 9 § får ske om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om bevarande och vård av arkiv.

Bemyndigande

12 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om i vilka fall andra än myndigheter får behandla sådana personuppgifter som avses i 9 §.

Personnummer och samordningsnummer

13 § Uppgifter om personnummer eller samordningsnummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

14 § Regeringen får meddela ytterligare föreskrifter om i vilka fall behandling av personnummer och samordningsnummer är tillåten.

4 kap. Användningsbegränsningar

Arkiverade personuppgifter

1 § Personuppgifter som behandlas enbart för arkivändamål av allmänt intresse får inte användas för att vidta åtgärder i fråga om den registrerade, annat än om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen.

Begränsningen i första stycket hindrar dock inte myndigheter från att använda personuppgifter som finns i allmänna handlingar.

Statistikuppgifter

2 § Personuppgifter som behandlas enbart för statistiska ändamål får inte användas för att vidta åtgärder i fråga om den registrerade, annat än om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen.

5 kap. Begränsningar av vissa rättigheter och skyldigheter

Information och tillgång till personuppgifter

1 § Den registrerades rätt till information och tillgång till personuppgifter enligt artiklarna 13–15 i dataskyddsförordningen gäller inte sådana uppgifter som den personuppgiftsansvarige inte får lämna ut till den registrerade enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning.

Om den personuppgiftsansvarige inte är en myndighet gäller undantaget i första stycket även för uppgifter som hos en myndighet

skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen (2009:400).

2 § Bestämmelsen om den registrerades rätt till tillgång till personuppgifter i artikel 15 i dataskyddsförordningen gäller inte personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande.

Undantaget i första stycket gäller inte om personuppgifterna

1. har lämnats ut till tredje part,
2. behandlas enbart för arkivändamål av allmänt intresse eller statistiska ändamål eller,
3. har behandlats under längre tid än ett år i löpande text som inte fått sin slutliga utformning.

Bemyndigande

3 § Regeringen får meddela föreskrifter om ytterligare begränsningar av vissa rättigheter och skyldigheter enligt artikel 23 i dataskyddsförordningen.

6 kap. Tillsynsmyndighetens handläggning och beslut

Befogenheter

1 § De befogenheter som tillsynsmyndigheten har enligt artikel 58.1, 58.2 och 58.3 i dataskyddsförordningen gäller även vid tillsyn över efterlevnaden av bestämmelserna i denna lag och andra författningar som kompletterar dataskyddsförordningen.

Ansökan hos allmän förvaltningsdomstol

2 § Om tillsynsmyndigheten vid handläggningen av ett ärende finner att det finns skäl att ifrågasätta giltigheten av en unionsrättsakt som påverkar tillämpningen av dataskyddsförordningen i ärendet, får tillsynsmyndigheten hos allmän förvaltningsdomstol ansöka om att en åtgärd enligt artikel 58.2 i dataskyddsförordningen ska vidtas.

Ansökan ska göras hos den förvaltningsrätt som är behörig att pröva ett överklagande av tillsynsmyndighetens beslut.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Kommunikation

3 § Innan tillsynsmyndigheten fattar ett beslut som avses i artikel 58.2 i dataskyddsförordningen, ska den som beslutet gäller ges tillfälle att inom en bestämd tid yttra sig över allt material av betydelse för beslutet, om det inte är uppenbart obehövt.

Om saken är brådskande får myndigheten, i avvaktan på yttrandet, besluta att behandlingen av personuppgifter tillfälligt ska begränsas eller förbjudas i enlighet med artikel 58.2 f i dataskyddsförordningen. Det tillfälliga beslutet ska omprövas, när tiden för yttrande har gått ut.

Delgivning

4 § Ett beslut som avses i 3 § första stycket ska delges, om det inte är uppenbart obehövt. Delgivning enligt 34–37 §§ delgivningslagen (2010:1932) får användas endast om det finns särskild anledning att anta att mottagaren har avvikit eller på annat sätt håller sig undan.

Besked angående handläggningen av ett klagomål

5 § Om tillsynsmyndigheten inte inom tre månader från den dag då ett klagomål kom in till myndigheten har behandlat klagomålet, ska tillsynsmyndigheten på skriftlig begäran av den registrerade antingen lämna besked i frågan om myndigheten avser att utöva tillsyn med anledning av klagomålet, eller i ett särskilt beslut avslå begäran om besked.

Besked eller beslut enligt första stycket ska meddelas inom två veckor från den dag då begäran om besked kom in till myndigheten.

Om tillsynsmyndigheten har avslagit en begäran om besked enligt första stycket, har den registrerade inte rätt till ett nytt besked i ärendet förrän tidigast tre månader efter det att myndighetens beslut meddelades.

7 kap. Administrativa sanktionsavgifter

1 § Sanktionsavgift får tas ut av en myndighet vid överträdelser som avses i artikel 83.4, 83.5 och 83.6 i dataskyddsförordningen, varvid artikel 83.1, 83.2 och 83.3 i förordningen ska tillämpas.

Vid överträdelser som avses i artikel 83.4 i dataskyddsförordningen ska avgiften bestämmas till högst 10 000 000 kronor och annars till högst 20 000 000 kronor.

2 § Sanktionsavgift får tas ut vid överträdelser av artikel 10 i dataskyddsförordningen, varvid artikel 83.1, 83.2 och 83.3 i förordningen ska tillämpas. Avgiftens storlek ska bestämmas med tillämpning av artikel 83.5 i förordningen.

3 § Sanktionsavgift får inte beslutas, om den som avgiften ska tas ut av inte har fått tillfälle att yttra sig enligt 6 kap. 3 § inom fem år från den dag då överträdelserna ägde rum.

4 § En sanktionsavgift som beslutats enligt dataskyddsförordningen eller denna lag tillfaller staten.

8 kap. Skadestånd och rättsmedel

Skadestånd

1 § Rätten till ersättning enligt artikel 82 i dataskyddsförordningen gäller även vid överträdelser av bestämmelser i denna lag och andra författningar som kompletterar dataskyddsförordningen.

Överklagande av beslut som fattats av en myndighet i egenskap av personuppgiftsansvarig

2 § Beslut enligt artiklarna 12.5, 15–19 eller 21 i dataskyddsförordningen som har meddelats av en myndighet i egenskap av personuppgiftsansvarig får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Första stycket gäller inte beslut av riksdagen, regeringen, Högsta domstolen, Högsta förvaltningsdomstolen eller riksdagens ombudsmän.

Dröjsmålstalan

3 § Tillsynsmyndighetens beslut att avslå en begäran om besked enligt 6 kap. 5 § får överklagas till allmän förvaltningsdomstol.

Om domstolen bifaller överklagandet, ska den förelägga tillsynsmyndigheten att inom en bestämd tid lämna besked till den registrerade i frågan om tillsyn kommer att utövas.

Domstolens beslut får inte överklagas.

Överklagande av tillsynsmyndighetens beslut

4 § Tillsynsmyndighetens beslut enligt dataskyddsförordningen och enligt 7 kap. 1 och 2 §§ denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagande av beslut i enskilda fall

5 § Beslut enligt 2 kap. 5 § andra stycket, 3 kap. 6 § tredje stycket och 3 kap. 10 § denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagandeförbud

6 § Andra beslut enligt denna lag än de som avses i 2–5 §§ och 6 kap. 2 § får inte överklagas.

1. Denna lag träder i kraft den 25 maj 2018.

2. Genom lagen upphävs personuppgiftslagen (1998:204).

3. Den upphävda lagen gäller dock fortfarande i den utsträckning som det i en annan lag eller förordning finns bestämmelser som innehåller hänvisningar till den lagen.

4. Äldre föreskrifter gäller fortfarande för ärenden hos Datainspektionen som har inletts men inte avgjorts före ikraftträdandet.

5. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats med stöd av dessa föreskrifter.

6. Äldre föreskrifter om skadestånd gäller fortfarande för skada som har orsakats före ikraftträdandet.

7. Äldre föreskrifter gäller fortfarande för överträdelser som har skett före ikraftträdandet.

1.2 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs att 10 kap. 27 §, 21 kap. 7 § och 40 kap. 5 § samt rubriken närmast före 21 kap. 7 § offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

10 kap.

27 §¹

Utöver vad som följer av 2, 3, 5 och 15–26 §§ får en sekretessbelagd uppgift lämnas till en myndighet, om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

Första stycket gäller inte i fråga om sekretess enligt 24 kap. 2 a och 8 §§, 25 kap. 1–8 §§, 26 kap. 1–6 §§, 29 kap. 1 och 2 §§, 31 kap. 1 § första stycket, 2 och 12 §§, 33 kap. 2 §, 36 kap. 3 § samt 40 kap. 2 och 5 §§.

Första stycket gäller inte heller om utlämnandet strider mot lag eller förordning *eller föreskrift som har meddelats med stöd av personuppgiftslagen (1998:204)*.

Första stycket gäller inte heller om utlämnandet strider mot lag eller förordning.

21 kap.

Behandling i strid med *personuppgiftslagen*

Behandling i strid med *dataskyddsregleringen*

7 §

Sekretess gäller för personuppgift, om det kan antas att ett utlämnande *skulle medföra att uppgiften* behandlas i strid med *personuppgiftslagen (1998:204)*.

Sekretess gäller för personuppgift, om det kan antas att *uppgiften efter* ett utlämnande *kommer att* behandlas i strid med *Europaparlamentets och rådets förordning (EU) 2016/679 av den*

¹ Senaste lydelse 2013:795.

27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), i den ursprungliga lydelsen, eller lagen (2018:xx) med kompletterande bestämmelser till EU:s dataskyddsförordning.

40 kap.

5 §

Sekretess gäller i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning av personuppgifter som avses i *personuppgiftslagen (1998:204)* för uppgift om en *enskilds personliga eller ekonomiska förhållanden*.

Sekretess gäller för uppgift om en *enskilds personliga eller ekonomiska förhållanden* i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning av sådana personuppgifter som avses i *artikel 4.1 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)*.

Denna lag träder i kraft den 25 maj 2018.

1.3 Förslag till förordning om ändring i arkivförordningen (1991:446)

Regeringen föreskriver i fråga om arkivförordningen (1991:446) dels att 7 a och 20 §§ ska ha följande lydelse, dels att det ska införas tre nya paragrafer, 7 b, 7 c och 7 d §§, av följande lydelse.

Nuvarande lydelse

En arkivmyndighet behöver inte lämna *besked* och information enligt 26 § *personuppgiftslagen* (1998:204) när det gäller personuppgifter i arkivmaterial som tagits emot för förvaring av myndigheten, om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

Föreslagen lydelse

7 a §²

En arkivmyndighet behöver inte lämna *bekräftelse, tillgång till personuppgifter* och information enligt *artikel 15 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)*, när det gäller personuppgifter i arkivmaterial som tagits emot för förvaring av myndigheten, om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

7 b §

En arkivmyndighet behöver inte rätta eller komplettera personuppgifter enligt artikel 16 i förordning (EU) 2016/679, när det gäller personuppgifter i arkivmate-

² Senaste lydelse 2001:556.

rial som tagits emot för förvaring av myndigheten.

7 c §

En arkivmyndighet behöver inte begränsa behandlingen av personuppgifter enligt artikel 18 i förordning (EU) 2016/679, när det gäller personuppgifter i arkivmaterial som tagits emot för förvaring av myndigheten.

7 d §

Rätten att göra invändningar enligt artikel 21 i förordning (EU) 2016/679 gäller inte vid en arkivmyndighets behandling av personuppgifter i arkivmaterial som tagits emot för förvaring av arkivmyndigheten.

20 §³

I 22 a § förvaltningslagen (1986:223) finns bestämmelser om överklagande hos allmän förvaltningsdomstol. Andra beslut än beslut enligt 7 a § får dock inte överklagas.

I 22 a § förvaltningslagen (1986:223) finns bestämmelser om överklagande hos allmän förvaltningsdomstol. Andra beslut än beslut enligt 7 a, 7 b, 7 c och 7 d §§ får dock inte överklagas.

Denna förordning träder i kraft den 25 maj 2018.

³ Senaste lydelse 2001:556.

1.4 Förslag till förordning med kompletterande bestämmelser till EU:s dataskyddsförordning

Regeringen föreskriver följande.

Inledande bestämmelser

1 § I denna förordning finns bestämmelser som kompletterar Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), nedan kallad dataskyddsförordningen.

Kompletterande bestämmelser finns också i lagen (2018:xx) med kompletterande bestämmelser till EU:s dataskyddsförordning, nedan kallad dataskyddslagen.

Termer och uttryck som används i denna förordning har samma betydelse som i dataskyddsförordningen och dataskyddslagen.

2 § Denna förordning är meddelad med stöd av

- 3 kap. 12 § dataskyddslagen i fråga om 4 § och 5 § första stycket,
- 3 kap. 10 § dataskyddslagen i fråga om 5 § andra stycket,
- 2 kap. 5 § och 3 kap. 6 § dataskyddslagen i fråga om 6 §, och
- 8 kap. 7 § regeringsformen i fråga om övriga bestämmelser.

Tillsynsmyndighet

3 § Datainspektionen är tillsynsmyndighet enligt dataskyddsförordningen och dataskyddslagen.

Personuppgifter som rör lagöverträdelser

4 § Personuppgifter som rör fällande domar i brottmål, lagöverträdelser som innefattar brott eller straffprocessuella tvångsmedel får behandlas av andra än myndigheter om

1. behandlingen är nödvändig för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras i ett enskilt fall,
2. behandlingen avser enstaka uppgifter och är nödvändig för att till polisen anmäla misstanke om brott, eller
3. behandlingen avser enstaka uppgifter och är nödvändig för att en rättslig förpliktelse enligt lag eller förordning ska kunna fullgöras.

5 § Datainspektionen får meddela ytterligare föreskrifter om i vilka fall andra än myndigheter får behandla personuppgifter som rör fäl-lande domar i brottmål, lagöverträdelser som innefattar brott eller straffprocessuella tvångsmedel.

Datainspektionen får även i enskilda fall besluta om att tillåta behandling av sådana personuppgifter som avses i första stycket.

Enskilda arkiv

6 § Riksarkivet får meddela föreskrifter om behandling av person-uppgifter för arkivändamål av allmänt intresse, när det gäller andra enskilda organ än de som omfattas av bestämmelserna om allmänna handlingar och sekretess i tryckfrihetsförordningen och offentlig-hets- och sekretesslagen (2009:400). Sådana föreskrifter får även avse behandling av känsliga personuppgifter.

Riksarkivet får även i enskilda fall besluta att sådana enskilda organ som avses i första stycket får behandla personuppgifter för arkiv-ändamål av allmänt intresse. Sådana beslut får även avse behandling av känsliga personuppgifter.

7 § Innan Riksarkivet meddelar föreskrifter eller fattar beslut enligt 6 § ska Datainspektionen ges tillfälle att yttra sig över Riksarkivets förslag.

Verkställighet av beslut om sanktionsavgift

8 § Sanktionsavgifter ska betalas till X-myndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom den tid som anges i första stycket, ska myndigheten lämna den obetalda avgiften för indrivning.

Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

9 § En beslutad sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom tio år från det att beslutet fick laga kraft.

10 § Om betalningsansvaret har upphävts genom ett beslut som fått laga kraft, ska sanktionsavgiften återbetalas. För sanktionsavgift som återbetalas utgår ränta enligt 5 § räntelagen (1975:635) för tiden från den dag då avgiften betalades till och med den dag den återbetalas.

Övriga verkställighetsföreskrifter

11 § Datainspektionen får meddela närmare föreskrifter om

1. klagomål till tillsynsmyndigheten, och
2. begäran om besked rörande handläggningen av klagomål.

1. Denna förordning träder i kraft den 25 maj 2018.

2. Genom förordningen upphävs personuppgiftsförordningen (1998:1191).

3. Den upphävda förordningen gäller dock fortfarande i den utsträckning som det i en annan lag eller förordning finns bestämmelser som innehåller hänvisningar till den förordningen.

4. Äldre föreskrifter gäller fortfarande för ärenden som har inletts hos Datainspektionen före ikraftträdandet men ännu inte har avgjorts.

5. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats med stöd av dessa föreskrifter.

2 Vårt uppdrag och arbete

2.1 Uppdraget

Vårt uppdrag har varit att föreslå de anpassningar och kompletterande författningsbestämmelser som den nya dataskyddsförordningen ger anledning till på generell nivå, samt att upphäva den nuvarande generella personuppgiftsregleringen.

I kommittédirektiven beskrivs vilken reglering som måste antas på nationell nivå, dvs. behövliga författningsförslag. Uppräkningen av dessa punkter är avsedd att vara uttömmande. Dessutom beskrivs i direktiven ett antal frågor där vi ska lämna lämpliga författningsförslag. I dessa fall finns det i dataskyddsförordningen inget krav på nationell reglering, men möjligheten finns. Utredningens direktiv finns i bilaga 1.

2.2 Avgränsningar

Vårt uppdrag har varit omfattande, samtidigt som de i direktiven givna tidsramarna måste hållas. Vi har mot den bakgrunden ansett det nödvändigt att tolka vårt uppdrag tämligen strikt och inte ta oss an uppgifter som inte klart framgår av de direktiv som lämnats till oss.

Utgångspunkten för vårt arbete har varit att endast utreda och lämna förslag till de anpassningar av nationell rätt som dataskyddsförordningen ger anledning till på ett generellt plan. I detta arbete har vi strävat efter att sådan personuppgiftsbehandling som är tillåten i dag i möjligaste mån ska kunna fortsätta. Vårt arbete har alltså inte syftat till att vare sig utvidga eller inskränka möjligheterna till behandling av personuppgifter, annat än då dataskyddsförordningen kräver en sådan förändring. Vi har inte haft i uppdrag att analysera eller beskriva vilka förändringar som dataskyddsförordningen i sig innebär

för möjligheten att behandla, och skyldigheten att skydda, personuppgifter. Det har inte heller varit vår uppgift att bedöma konsekvenserna av förordningens direkt tillämpliga bestämmelser eller av de förändringar som dessa innebär.

I uppdraget har inte ingått att överväga eller lämna förslag till grundlagsändringar. Uppdraget har inte heller omfattat att se över eller lämna förslag till förändringar av sådan sektorsspecifik reglering om behandling av personuppgifter som bland annat finns i de särskilda registerförfattningarna. Vi har således inte utrett frågor som endast rör vissa typer av verksamheter. Några av de frågor som beskrivs i kommittédirektiven och som behandlats i vår utredning är dock av relevans enbart för den offentliga sektorn, men då på ett generellt plan. Flertalet frågor rörande tillsynsmyndigheten har inte ingått i vår utredning, utan har i stället omhändertagits av Utredningen av tillsynen över den personliga integriteten (Ju 2015:02).

Efter det att våra direktiv beslutades har regeringen gett en särskild utredare i uppdrag att bland annat analysera vilken reglering av personuppgiftsbehandling för forskningsändamål som är möjlig och kan behövas, utöver den generella reglering som vi kommer att föreslå, och att analysera vilka anpassningar av lagen (2003:460) om etikprövning av forskning som avser människor som behöver göras. Utredningen har tagit namnet Forskningsdatautredningen (U 2016:04). Vi har i samråd med Forskningsdatautredningen konstaterat att samtliga frågor rörande behandling av personuppgifter för forskningsändamål bör behandlas i ett samlat sammanhang och att Forskningsdatautredningen är bäst lämpad att göra den analys och de överväganden som krävs. Vi har därför avstått från att i vårt arbete behandla frågan om behandling av personuppgifter för forskningsändamål.

2.3 Utredningsarbetet

Utredningsarbetet har bedrivits på sedvanligt sätt med regelbundna expertgruppsammanträden. Utredningen har sammanträtt med de förordnade experterna och den sakkunniga vid sammanlagt elva tillfällen. Utredningsarbetet har även i övrigt bedrivits i nära samarbete med experterna och den sakkunniga.

Utredaren och sekreterarna samrådde med Utredningen om 2016 års dataskyddsdirektiv (Ju 2016:06) den 15 april 2016 inför pla-

neringen av utredningsarbetet. Utredarna har därefter samrått vid flera tillfällen. Sekreterarna har haft fortlöpande kontakter med varandra i för utredningarna gemensamma frågor. Den mycket begränsade tiden för vårt utredningsarbete har dock inte lämnat utrymme för att i tillräcklig utsträckning ta del av Utredningens om 2016 års dataskyddsdirektiv förslag och texter. Det kan därför finnas oavsiktliga skillnader mellan utredningarnas syn på likartade frågor.

Parallellt med vår utredning har ett flertal andra utredningar också haft i uppdrag att anpassa svensk rätt till dataskyddsreformen. Vi har tillsammans med dessa andra utredningar ingått i en informell samordningsgrupp. Under utredningstiden har det hållits nio möten i denna samordningsgrupp. Vi har löpande under utredningstiden delat våra texter med samordningsgruppen, men har däremot inte haft tid att ta del av de andra utredningarnas texter. Det kan därför även i förhållande till dessa utredningar finnas oavsiktliga skillnader i synen på likartade frågor.

Vid sidan av samarbetet med Utredningen om 2016 års dataskyddsdirektiv och inom samordningsgruppen har vi dessutom löpande under utredningsarbetet samrått och haft kontakter med bland andra Utredningen om tillsynen över den personliga integriteten (Ju 2015:02) och Utredningen om kameraövervakningslagen – brottsbekämpning och integritetsskydd (Ju 2015:14).

Den 24 oktober 2016 närvarade vi vid konferensen Nordic Privacy Arena, som anordnades av organisationen Forum för dataskydd. Vi har även deltagit i ett seminarium i riksdagen den 8 december 2016 om ”Åldersgräns för sociala medier – skydd eller begränsning av barn och ungas rättigheter?”, som anordnades av organisationen Surfa lugnt. Vi har också deltagit i ett nordiskt samrådsmöte i Köpenhamn den 12 december 2016, anordnat av Nordiska ministerrådet. Vidare har vi under utredningstiden haft en dialog med Riksarkivet om frågor som rör behandling av personuppgifter för arkivändamål.

Slutligen har vi gett Statens medieråd och Barnombudsmannen tillfälle att lämna yttranden när det gäller frågan om barns samtycke till personuppgiftsbehandling vid erbjudandet av informationssamhällets tjänster direkt till barn. Svar har inkommit från båda dessa myndigheter.

3 Gällande rätt

3.1 Inledning

Begreppet personlig integritet används i vardagligt tal vanligen för att beteckna individens värde och värdighet. Begreppet finns både i grundlag och i vanlig lag. Någon allmängiltig definition av begreppet har dock inte slagits fast i lagstiftningen. I ett försök att ändå beskriva vad som kan anses vara kärnan i rätten till personlig integritet har regeringen uttalat att kränkningar av den personliga integriteten utgör intrång i den fredade sfär som den enskilde bör vara tillförsäkrad och där ett oönskat intrång bör kunna avvisas.¹

I dagens samhälle behandlas stora mängder personuppgifter elektroniskt av både privata och offentliga aktörer. Det är nödvändigt för att företag ska kunna bedriva en konkurrenskraftig affärsverksamhet och för att offentliga organ ska kunna utföra sina uppdrag på ett effektivt och rättssäkert sätt. Denna hantering är dock förenad med påtagliga risker. Om de personuppgifter som samlats in utnyttjas för andra syften än avsett eller annars behandlas på ett otillbörligt sätt, eller om uppgifterna på grund av säkerhetsbrister hamnar i fel händer, kan det leda till allvarlig skada för enskildas personliga integritet. För att skydda enskildas integritet har det därför ansetts finnas ett behov av bestämmelser som bland annat begränsar hur, när och varför personuppgifter får behandlas och som reglerar hur otillåten behandling ska förhindras och beivras.

I detta kapitel beskrivs kortfattat den övergripande rättsliga regleringen till skydd för den personliga integriteten, i den mån denna reglering är av relevans med avseende på behandling av personuppgifter.

¹ Prop. 2009/10:80 s. 175, och prop. 2005/06:173 s. 15. För en genomgång av integritetsbegreppet i tidigare utredningsarbete, se SOU 2016:7 s. 69 f.

3.2 Internationella överenskommelser

3.2.1 Förenta Nationerna

Förenta Nationerna (FN) antog 1948 den allmänna förklaringen om de mänskliga rättigheterna. Förklaringen är inte formellt bindande för medlemsstaterna, men ses som ett uttryck för sedvane-
rättsliga regler. Skyddet för den personliga integriteten behandlas i artikel 12, som anger att ingen må utsättas för godtyckligt ingripande i fråga om privatliv, familj, hem eller korrespondens och inte heller för angrepp på sin heder eller sitt anseende. Var och en har rätt till lagens skydd mot sådana ingripanden och angrepp. I artikel 29 anges att en person endast får underkastas sådana inskränkningar som har fastställts i lag och enbart i syfte att trygga tillbörlig hänsyn till och respekt för andras rättigheter och friheter samt för att tillgodose ett demokratiskt samhälles berättigade krav på moral, allmän ordning och allmän välfärd.

Inom FN har också utarbetats en internationell konvention om medborgerliga och politiska rättigheter, som antogs av generalförsamlingen 1966 och trädde i kraft 1976. Sverige anslöt sig till konventionen 1971. I artikel 17 återupprepas vad som anges i artikel 12 i den allmänna förklaringen.

FN:s generalförsamling antog 1990 riktlinjer om datoriserade register med personuppgifter. I riktlinjerna finns tio grundläggande principer som medlemsstaterna ska ta hänsyn till vid lagstiftning avseende datoriserade register med personuppgifter. Det anges bland annat att personuppgifter inte får samlas in eller behandlas i strid med FN:s stadga.

3.2.2 OECD

Inom Organisationen för ekonomiskt samarbete och utveckling, OECD, har en expertgrupp utarbetat riktlinjer i fråga om integritetsskyddet och personuppgiftsflödet över gränserna. Riktlinjerna antogs 1980 av OECD:s råd tillsammans med en rekommendation till medlemsländernas regeringar om att betrakta riktlinjerna i nationell lagstiftning. Riktlinjerna reviderades år 2013. Samtliga medlemsländer, däribland Sverige, har godtagit rekommendationen och åtagit sig att följa denna.

Riktlinjerna ska uppfattas som minimiregler och motsvarar i princip de bestämmelser som finns i Europarådets dataskyddskonvention, se nedan. De är tillämpliga på behandling av personuppgifter inom både den privata och den offentliga sektorn.

3.3 Europarätt

3.3.1 Europarådet

Europakonventionen

Sedan den 1 januari 1995 är den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) inkorporerad i svensk rätt och gäller som lag². Av 2 kap. 19 § regeringsformen framgår att lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden på grund av konventionen.

Enligt artikel 8 i Europakonventionen har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Offentlig myndighet får inte inskränka åtnjutande av denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välbefinnande eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.

Behandling av personuppgifter kan falla inom tillämpningsområdet för artikel 8 i Europakonventionen i de fall behandlingen avser uppgifter om privatliv, familjeliv, hem eller korrespondens. EU-domstolen har slagit fast att bestämmelserna i artikel 8 i Europakonventionen har viss betydelse vid bedömningen av nationella regler som tillåter behandling av personuppgifter.³ Vidare har EU-domstolen slagit fast att artikel 8 i Europakonventionen ålägger staten såväl en negativ förpliktelse att avstå från att göra intrång i rätten till respekt för privat- och familjelivet som en positiv för-

² Lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna, prop. 1993/94:117.

³ Dom Österreichischer Rundfunk m.fl., C-465/00, C-138/01 och C-139/01, EU:C:2003:294.

pliktelse att skydda enskilda mot att andra enskilda handlar på ett sätt som innebär integritetsintrång.⁴

Dataskyddskonventionen

Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter, den s.k. dataskyddskonventionen, antogs av Europarådets ministerkommitté 1981. Konventionen trädde i kraft den 1 oktober 1985. Samtliga medlemsstater i EU har ratificerat konventionen.

Konventionens syfte är att säkerställa respekten för grundläggande fri- och rättigheter, särskilt den enskildes rätt till personlig integritet i samband med automatiserad behandling av personuppgifter. Konventionen tar sikte på behandling av personuppgifter i automatiserade personregister och automatiserad personuppgiftsbehandling i allmän och enskild verksamhet. Personuppgifterna ska enligt konventionen inhämtas och behandlas på ett korrekt sätt och de ska vara relevanta med hänsyn till ändamålet. Vissa kategorier av personuppgifter får inte behandlas genom automatiserad databehandling om inte den nationella lagstiftningen ger ett ändamålsenligt skydd. Till sådana kategorier hör personuppgifter som avslöjar ras, politisk tillhörighet, religiös tro eller övertygelse i övrigt, sexualliv samt uppgifter om brott. En översyn av konventionen pågår för närvarande inom Europarådet.

Det har inom Europarådet även utarbetats flera rekommendationer på dataskyddsområdet. Dessa är dock, till skillnad från dataskyddskonventionen, inte bindande.

3.3.2 Europeiska unionen

Stadgan

Vid Europeiska rådets möte i Nice år 2000 antog EU:s medlemsstater Europeiska unionens stadga om de grundläggande rättigheterna. Som en följd av Lissabonfördraget, som trädde i kraft år

⁴ Se t.ex. Airey mot Irland, nr 6289/73, dom den 9 oktober 1979, X och Y mot Nederländerna, nr 8978/80, dom den 26 mars 1985, K.U. mot Finland, nr 2872/02, dom den 2 december 2008 och Söderman mot Sverige, nr 5786/08, dom den 12 november 2013.

2009, är stadgan rättsligt bindande för EU-institutionerna och medlemsstaterna när dessa tillämpar unionsrätten.

I artikel 7 i stadgan anges att var och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Av artikel 8 i stadgan framgår vidare att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. En oberoende myndighet ska kontrollera att dessa regler efterlevs.

Dataskyddsdirektivet och dataskyddsrambeslutet

Den allmänna regleringen om behandling av personuppgifter inom EU finns i dag i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet). Direktivet syftar till att garantera en hög och i alla medlemsstater likvärdig skyddsnivå när det gäller enskilda personers fri- och rättigheter med avseende på behandling av personuppgifter, samt att främja ett fritt flöde av personuppgifter mellan medlemsstaterna i EU.

Dataskyddsdirektivet gäller inte för behandling av personuppgifter på områden som faller utanför unionsrätten, till exempel allmän säkerhet och försvar samt statens verksamhet på straffrättens område. Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet) är, som namnet antyder, tillämpligt på informationsutbyte över gränserna. Data-skyddsrambeslutet gäller däremot inte för rent nationell personuppgiftsbehandling inom exempelvis polisens område. Från data-skyddsrambeslutets tillämpningsområde undantas också personuppgiftsbehandling inom området nationell säkerhet. På detta område finns det således inte någon EU-gemensam reglering avseende behandling av personuppgifter.

3.4 Svensk rätt

3.4.1 Regeringsformen

Svensk grundlag ger ett grundläggande skydd för den personliga integriteten, utöver det som följer av att lag eller annan föreskrift inte får meddelas i strid med Europakonventionen. Enligt målsättningsstadgandet i 1 kap. 2 § första stycket regeringsformen ska den offentliga makten utövas med respekt för den enskilda människans frihet. I fjärde stycket samma paragraf anges att det allmänna ska värna om den enskildes privat- och familjeliv. I 2 kap. 4 och 5 §§ regeringsformen finns bestämmelser om absolut skydd mot allvarliga fysiska integritetsintrång, bland annat döds- och kroppsstraff. Enligt 2 kap. 6 § första stycket regeringsformen är var och en därutöver skyddad gentemot det allmänna mot bland annat påtvingade kroppsliga ingrepp.

För att stärka skyddet för den personliga integriteten infördes den 1 januari 2011 ett nytt andra stycke i 2 kap. 6 § regeringsformen. I bestämmelsen anges att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Skyddet får enligt 2 kap. 20 och 21 §§ regeringsformen begränsas genom lag, men endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningen får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar. Begränsningen får inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning.

3.4.2 Dataskyddsdirektivets genomförande

Dataskyddsdirektivet har genomförts i svensk rätt huvudsakligen genom personuppgiftslagen (1998:204), förkortad PUL. Bestämmelserna i personuppgiftslagen har till syfte att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Personuppgiftslagen följer i princip dataskyddsdirektivets struktur och innehåller liksom direktivet bestämmelser

om bland annat personuppgiftsansvar, grundläggande krav för behandling av personuppgifter och information till den registrerade.

Personuppgiftslagen är tillämplig även utanför EU-rättens område och gäller både för myndigheter och enskilda som behandlar personuppgifter. Personuppgiftslagen är samtidigt subsidiär, vilket innebär att lagens bestämmelser inte ska tillämpas om det finns avvikande bestämmelser i en annan lag eller förordning. Det finns en stor mängd sådana bestämmelser i sektorsspecifika författningar som främst reglerar hur olika myndigheter får behandla personuppgifter.

Personuppgiftslagen kompletteras också av bestämmelser i personuppgiftsförordningen (1998:1191), förkortad PUF, som bland annat pekar ut Datainspektionen som tillsynsmyndighet. Datainspektionen bemyndigas i förordningen att meddela närmare föreskrifter om bland annat i vilka fall behandling av personuppgifter är tillåten och vilka krav som ställs på den personuppgiftsansvarige.

4 EU:s dataskyddsreform

4.1 Allmänt om reformen

I artikel 16 i fördraget om Europeiska unionens funktionssätt, som trädde i kraft år 2009 genom Lissabonfördraget, anges att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Vidare anges att Europaparlamentet och rådet i enlighet med det ordinarie lagstiftningsförfarandet ska fastställa bestämmelser om skydd för enskilda personer när det gäller behandling av personuppgifter hos unionens institutioner, organ och byråer och i medlemsstaterna, när dessa utövar verksamhet som omfattas av unionsrättens tillämpningsområde, samt om den fria rörligheten för sådana uppgifter.

Bestämmelsen ger unionen befogenhet att anta rättsakter om skydd för personuppgifter inom hela tillämpningsområdet för unionsrätten, med vissa särbestämmelser för den gemensamma utrikes- och säkerhetspolitiken avseende behandling av personuppgifter i medlemsstaterna. EG:s befogenheter på området omfattade endast den första pelaren. Genom Lissabonfördraget har således befogenheterna att anta rättsakter till skydd för den personliga integriteten utvidgats.

Kommissionen lade fram sitt förslag till en reformerad dataskyddsreglering i EU år 2012. Förslaget avsåg dels en förordning med allmänna EU-regler om skydd av personuppgifter som skulle ersätta dataskyddsdirektivet, och dels ett direktiv med regler om skydd av personuppgifter som behandlas i samband med förebyggande, utredning, avslöjande eller lagföring av brott och därmed förbunden rättslig verksamhet som skulle ersätta dataskyddsrambeslutet.¹ En politisk

¹ Förslag till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning) (COM[2012] 11 final av den 25 januari 2012) och Förslag till Europaparlamentets och rådets direktiv om skydd för enskilda personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter (COM[2012] 10 final av den 25 januari 2012).

överenskommelse om regleringen kunde nås den 15 december 2015. Enligt kommissionens pressmeddelande efter den politiska överenskommelsen var syftet med reformen i huvudsak att stärka enskildas befintliga rättigheter och se till att enskilda får mer kontroll över sina personuppgifter, men också att harmonisera EU:s regler om skydd av personuppgifter och därmed skapa affärsmöjligheter och främja innovation.²

4.2 Dataskyddsförordningen

Den 27 april 2016 antogs Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning). I dagligt tal används ofta den vedertagna engelska förkortningen, GDPR. Vi har dock valt att i detta betänkande benämna den nya rättsakten *dataskyddsförordningen* eller kort och gott *förordningen*.

Dataskyddsförordningen kommer från och med den 25 maj 2018 att ersätta det nuvarande dataskyddsdirektivet och utgöra den generella regleringen av personuppgiftsbehandling inom EU. Enligt artikel 288 andra stycket i fördraget om Europeiska unionens funktions sätt ska en EU-förordning ha allmän giltighet och vara till alla delar bindande och direkt tillämplig i varje medlemsstat. Till skillnad från EU-direktiv ska alltså förordningar inte implementeras i nationell rätt. I stället ska förordningsbestämmelser tillämpas av enskilda, myndigheter och domstolar precis som om de vore nationella författningsbestämmelser. Detta innebär att dataskyddsförordningen är direkt tillämplig.

Även om dataskyddsförordningen är direkt tillämplig, till skillnad från dataskyddsdirektivet, innehåller den många bestämmelser som förutsätter eller ger utrymme för kompletterande nationella bestämmelser av olika slag. Förordningen har därmed i vissa delar en direktivliknande karaktär. I skälen till förordningen anges också att om förordningen föreskriver förtydliganden eller begränsningar av dess

² Europeiska kommissionens pressmeddelande den 15 december 2015 "Överenskommelse om kommissionens reform av EU:s uppgiftsskydd stärker den digitala inre marknaden".

bestämmelser genom medlemsstaternas nationella rätt, kan medlemsstaterna, i den utsträckning det är nödvändigt för samstämmigheten och för att göra de nationella bestämmelserna begripliga för de personer som de tillämpas på, införliva delar av förordningen i nationell rätt.

4.2.1 Förordningens syfte

I skälen till förordningen konstateras att dataskyddsdirektivet inte har kunnat förhindra bristande enhetlighet i genomförandet och tillämpningen av dataskyddet i olika delar av unionen. Skillnader i nivån på skyddet av personuppgifter kan enligt skälen förhindra det fria flödet av personuppgifter och kan därför utgöra ett hinder för att bedriva ekonomisk verksamhet på unionsnivå, snedvrیدا konkurrensen och hindra myndigheterna från att fullgöra sina skyldigheter enligt unionsrätten.

För att säkerställa en enhetlig skyddsnivå över hela unionen och undvika avvikelser som hindrar den fria rörligheten av personuppgifter inom den inre marknaden behövs, enligt skälen till förordningen, en förordning som skapar rättslig säkerhet och öppenhet för ekonomiska aktörer och som ger fysiska personer i alla medlemsstater samma rättsligt verkställbara rättigheter och skyldigheter samt ålägger personuppgiftsansvariga och personuppgiftsbiträden samma ansvar. På så sätt blir övervakningen av behandling av personuppgifter enhetlig, sanktionerna i alla medlemsstater likvärdiga och samarbetet mellan tillsynsmyndigheterna i olika medlemsstater effektivt.

4.2.2 Tillämpningsområdet

Dataskyddsförordningen ska, precis som dataskyddsdirektivet, tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.

Från dataskyddsförordningens tillämpningsområde undantas behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten eller som utförs av medlemsstaterna när de bedriver verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken. Behandling av personuppgifter som utförs av

en fysisk person som ett led i verksamhet av privat natur eller som har samband med hans eller hennes hushåll omfattas inte heller förordningens bestämmelser. Vidare gäller förordningen inte för sådan behandling av personuppgifter som utförs av behöriga myndigheter för ändamålen att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder. Sådan behandling regleras i stället genom det nya dataskyddsdirektivet, Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, som ersätter dataskyddsrambeslutet. Slutligen ska förordningens bestämmelser inte tillämpas av EU:s institutioner, organ och byråer. Den behandling av personuppgifter som sker där regleras i stället genom Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter. Ett förslag till reviderad förordning om skydd för personuppgifter som behandlas av unionens institutioner, organ, kontor och byråer har lagts fram av kommissionen.³

Dataskyddsförordningen ska tillämpas på all behandling av personuppgifter som sker inom ramen för den verksamhet som bedrivs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad i unionen, oavsett om behandlingen utförs i unionen eller inte. En skillnad jämfört med dataskyddsdirektivets ordalydelse är att förordningen under vissa omständigheter ska tillämpas även på behandling av personuppgifter som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad i unionen. Detta gäller om behandlingen avser registrerade som befinner sig i unionen, under förutsättning att behandlingen har anknytning till antingen utbudande av varor eller tjänster till sådana registrerade i unionen eller övervakning av deras beteende, så länge beteendet sker inom unionen. Slutligen ska dataskyddsförordningen också tillämpas på behandling av personuppgifter som utförs av en

³ COM (2017) 8 final, 2017/0002 (COD).

personuppgiftsansvarig som inte är etablerad i unionen, men på en plats där en medlemsstats nationella rätt gäller enligt folkrätten.

4.2.3 Sakliga förändringar

Dataskyddsförordningen baseras till stor del på dataskyddsdirektivets struktur och innehåll, men innebär även en rad förändringar. Några av dessa förtjänar att nämnas särskilt.

Den registrerades rättigheter har förstärkts i syfte att ge den registrerade ökad kontroll över sina personuppgifter. Den information som ska tillhandahållas den registrerade har preciserats och utvidgats och det anges uttryckligen att den personuppgiftsansvarige ska tillhandahålla informationen i en begriplig och lättillgänglig form. Förordningen innebär även en förstärkning av rätten att få åtkomst till sina personuppgifter i syfte att föra över dem till en annan leverantör av elektroniska tjänster, s.k. dataportabilitet. Vidare har en tydligare rätt till radering ("rätt att bli bortglömd") införts.

Det införs ett krav på att i vissa fall inhämta samtycke från vårdnadshavare eller godkännande av barnets samtycke när informationssamhällets tjänster erbjuds direkt till ett barn. Barns särställning och särskilda utsatthet poängteras på flera ställen i förordningen.

Genom förordningen införs en skyldighet för den personuppgiftsansvarige att anmäla till tillsynsmyndigheten om det inträffar en så kallad personuppgiftsincident, dvs. en säkerhetsincident som oavsiktligt påverkar behandlingen av personuppgifter. Även den registrerade ska informeras om incidenten om den sannolikt leder till en hög risk för enskildas rättigheter och friheter.

Det införs krav på konsekvensanalyser om en viss behandling sannolikt kommer att leda till hög risk för enskildas rättigheter eller skyldigheter. Den allmänna anmälningsskyldigheten till tillsynsmyndigheten tas däremot bort. Vidare blir det tydligare regler för kommunikation och ansvar hos de som behandlar personuppgifter. Ett krav på inbyggt dataskydd och dataskydd som standard införs.

Genom förordningen införs ett nytt gemensamt system med administrativa sanktionsavgifter som ska tas ut vid vissa typer av överträdelse av förordningen. Även på andra sätt innebär förordningen ett ökat fokus på en enhetlig tillämpning av dataskyddsreglerna inom EU, till exempel genom åtgärder som godkännande av

uppförandekoder och certifiering. Det införs även en skyldighet för de nationella tillsynsmyndigheterna att samarbeta med varandra. Det införs samtidigt en ny princip om en enda kontaktpunkt, som ska underlätta för sådana personuppgiftsansvariga som är verksamma i flera medlemsstater genom att de endast ska behöva vara i kontakt med en av de behöriga tillsynsmyndigheterna. Det kommer även att införas ett nytt unionsorgan, Europeiska dataskyddsstyrelsen, som får långtgående befogenheter att uttala sig om tolkningen av förordningen även i enskilda fall.

Förhållandet till offentlighetsprincipen

Utrymmet för att ge offentlighetsprincipen företräde framför personuppgiftsregleringen har blivit tydligare i förordningen, genom en uttrycklig och direkt tillämplig bestämmelse i artikel 86. Av bestämmelsen följer att personuppgifter i allmänna handlingar får lämnas ut i enlighet med nationell rätt, för att jämka samman allmänhetens rätt att få tillgång till handlingar med rätten till skydd för personuppgifter i enlighet med förordningen. Artikel 86 möjliggör alltså en tillämpning av tryckfrihetsförordningens reglering om allmänhetens tillgång till handlingar när det gäller allmänna handlingar som innehåller personuppgifter.

5 Ett nytt svenskt regelverk om dataskydd

5.1 Vårt uppdrag

Dataskyddsförordningen kommer att utgöra den generella regleringen av personuppgiftsbehandling inom EU. Detta innebär att personuppgiftslagen och anslutande föreskrifter måste upphävas. Vårt övergripande uppdrag är att föreslå en ny nationell reglering som på ett generellt plan kompletterar förordningen. En lag som kompletteras av bestämmelser i en nationell förordning samt en viss föreskriftsrätt för tillsynsmyndigheten kan enligt kommittédirektiven vara en lämplig utgångspunkt.

I kommittédirektiven anges att det vid utförandet av uppdraget är viktigt att – i den mån utrymme finns på nationell nivå – hitta lämpliga avvägningar mellan skyddet för den personliga integriteten samt myndigheters, företags och enskildas behov av att kunna behandla personuppgifter. I vårt uppdrag ingår dock inte att se över eller lämna förslag till förändringar av sådan sektorsspecifik reglering om behandling av personuppgifter som bland annat finns i de särskilda registerförfattningarna. Frågan om förhållandet mellan sektorsspecifik reglering och den kompletterande reglering som vi föreslår kan däremot aktualiseras. I uppdraget ingår därför att analysera om det finns behov att reglera förhållandet mellan den kompletterande regleringen och sektorsspecifika föreskrifter.

5.2 Överväganden och förslag

Utredningens förslag: Personuppgiftslagen och personuppgiftsförordningen ska upphävas. En ny lag och förordning med bestämmelser som kompletterar dataskyddsförordningen på ett generellt plan ska införas. Termer och uttryck i dessa författningar ska ha samma betydelse som i dataskyddsförordningen. Sektorsspecifika författningsbestämmelser som rör behandling av personuppgifter ska ha företräde framför den nya lagen.

5.2.1 Personuppgiftslagen, personuppgiftsförordningen och Datainspektionens föreskrifter ska upphävas

Dataskyddsförordningen ersätter dataskyddsdirektivet, som på generell nivå har genomförts i svensk rätt genom personuppgiftslagen, personuppgiftsförordningen och Datainspektionens föreskrifter. Dataskyddsförordningen ska däremot inte implementeras i svensk rätt, utan i stället tillämpas av enskilda, myndigheter och domstolar precis som om dess bestämmelser hade funnits i en svensk författning. När dataskyddsförordningen börjar tillämpas kommer alltså den generella regleringen om behandling av personuppgifter att finnas i dataskyddsförordningen. Det svenska generella regelverket om dataskydd kan då inte längre finnas kvar, eftersom det skulle leda till en otillåten dubbelreglering. Många av de bestämmelser som finns i personuppgiftslagen och i personuppgiftsförordningen motsvaras nämligen av direkt tillämpliga bestämmelser i dataskyddsförordningen.

Det ankommer på riksdagen att fatta beslut om upphävande av personuppgiftslagen, medan personuppgiftsförordningen bör upphävas genom regeringsbeslut. Datainspektionens föreskrifter som ansluter till personuppgiftslagen och personuppgiftsförordningen bör lämpligen upphävas av Datainspektionen, innan personuppgiftsförordningen upphör att gälla.

5.2.2 Ett regelverk som kompletterar dataskyddsförordningen på generell nivå ska införas

Den omständigheten att den nya generella unionsrättsakten om dataskydd är en förordning, och inte ett direktiv, innebär omfattande begränsningar av möjligheten att införa eller behålla nationella bestämmelser om dataskydd. Dataskyddsförordningen har emellertid i vissa delar en direktivliknande karaktär, på så sätt att ett förhållandevis stort antal artiklar förutsätter eller medger nationella bestämmelser som kompletterar eller föreskriver undantag från förordningens regler. I skäl 8 till förordningen anges också att om förordningen föreskriver förtydliganden eller begränsningar av dess bestämmelser genom medlemsstaternas nationella rätt, kan medlemsstaterna, i den utsträckning det är nödvändigt för samstämmigheten och för att göra de nationella bestämmelserna begripliga för de personer som de tillämpas på, införliva delar av förordningen i nationell rätt.

Vissa av de kompletterande bestämmelser som behövs eller är lämpliga är av generell karaktär, i betydelsen att de rör hela samhället eller flertalet myndigheter och inte bara en viss sektor. Denna typ av generella bestämmelser bör samlas i en ny övergripande lag och förordning om dataskydd. För att betona att författningarna inte är heltäckande, utan endast utgör ett komplement till dataskyddsförordningen, bör de benämnas *lagen med kompletterande bestämmelser till EU:s dataskyddsförordning* respektive *förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning*. I det följande kallar vi den nya lagen för dataskyddslagen.

Bestämmelser till skydd för den enskildes personliga integritet har vid normgivningen betraktats som offentlighetsrättsliga föreskrifter av den svenska lagstiftaren. Bestämmelserna utgör ett medel för det allmänna att skydda enskilda mot kränkning av deras personliga integritet genom olämplig behandling av personuppgifter. Genom tillsynsmyndigheten övervakar det allmänna att såväl privaträttsliga som offentlighetsrättsliga organ följer regelverket. Eventuella överträdelser kan beivras genom offentlighetsrättsliga sanktioner, förbud och begränsningar. Den omständigheten att överträdelser även kan föranleda civilrättsliga sanktioner i form av skadestånd förtar inte regleringen dess offentlighetsrättsliga karaktär.¹ Riksdagen kan därmed, enligt

¹ Prop. 1997/98:44 s. 58 f.

8 kap. 3 § regeringsformen, delegera sin normgivningskompetens på detta område till regeringen. Bestämmelser som meddelas med stöd av ett sådant bemyndigande kan dock aldrig läggas till grund för behandling som innebär sådan övervakning eller kartläggning av enskildas personliga förhållanden som avses i 2 kap. 6 § regeringsformen. Sådana betydande intrång i den personliga integriteten omfattas nämligen av ett särskilt lagkrav, enligt 2 kap. 20 § regeringsformen. De förordningsbestämmelser som vi föreslår är dock inte av denna karaktär.

Termer och uttryck

Många av de termer och uttryck som används i dataskyddsförordningen definieras i artikel 4 i förordningen. Andra begrepp definieras visserligen inte, men är av unionsrättslig karaktär och kan inte ges en särskild betydelse i nationell rätt. Termer och uttryck som används i den dataskyddslag och kompletterande förordning som vi föreslår bör därför ha samma betydelse som i dataskyddsförordningen. I övrigt innehåller våra författningsförslag inte några termer eller uttryck som kräver en reglerad definition.

Hänvisningsteknik

Den nya lag och förordning med kompletterande bestämmelser till dataskyddsförordningen som föreslås i detta betänkande innehåller hänvisningar till bestämmelser i EU-förordningen. Hänvisningar till EU-rättsakter kan göras antingen statiska eller dynamiska. En statisk hänvisning innebär att hänvisningen avser EU-rättsakten i en viss angiven lydelse. En dynamisk hänvisning innebär att hänvisningen avser EU-rättsakten i den vid varje tidpunkt gällande lydelsen.

Dataskyddsförordningen är direkt tillämplig. Handlingsutrymmet för medlemsstaterna när det gäller att införa bestämmelser i nationell rätt på detta område är därmed begränsat. För att säkerställa att ändringar i dataskyddsförordningen får omedelbart genomslag är det lämpligt att hänvisningarna dit görs dynamiska. Detta hindrar emellertid inte att dataskyddslagen och den kompletterande förordningen kan komma att behöva ändras om dataskyddsförordningens innehåll ändras. De hänvisningar till dataskyddsförordningen som finns i den

dataskyddslag och kompletterande förordning som föreslås i detta betänkande är därför med ett enda undantag dynamiska, dvs. avser förordningen i dess vid varje tidpunkt gällande lydelse. Hänvisningarna kommer således att omfatta även eventuella framtida ändringar i dataskyddsförordningen. Det är en hänvisningsteknik som regeringen ofta har använt i senare tids propositioner (se t.ex. prop. 2015/16:156 s. 20 f. och 33 f., prop. 2015/16:160 s. 36 f. och 45, prop. 2016/17:22 s. 96 f. och prop. 2016/17:125 s. 50).

Lagrådet har uttalat att en konsekvensanalys bör göras vid valet av hänvisningsteknik och redovisas för var och en av de hänvisningar som görs. Särskilt bör det enligt Lagrådet belysas hur det nationella regelsystemet faktiskt ändras genom hänvisningen och hur ändringar av rättsakten kan komma att påverka den nationella regleringen.²

Flera av hänvisningarna till dataskyddsförordningen i de bestämmelser som vi föreslår är av upplysande karaktär. Det gäller främst hänvisningarna i bestämmelserna om rättslig grund, känsliga personuppgifter och skadestånd. Dynamiska hänvisningar framstår som mest lämpligt i dessa fall. Detsamma gäller hänvisningarna till dataskyddsförordningen avseende betydelsen av de termer och uttryck som används i författningarna. Terminologin som används i den nationella reglering som kompletterar EU-förordningen måste följa den begreppsutveckling som sker inom unionen, även vid en eventuell ändring av uttryckliga definitioner i dataskyddsförordningen.

Andra hänvisningar till dataskyddsförordningen finns i föreslagna lag- och förordningsbestämmelser som rör bland annat vilka myndigheter eller andra aktörer som är behöriga att pröva olika frågor eller som har att vidta åtgärder enligt dataskyddsförordningen samt vilka förfarandebestämmelser som ska gälla när förordningen saknar bestämmelser eller hänvisar till att nationell rätt ska tillämpas. Data-skyddsförordningen innebär även att det i svensk rätt måste införas bestämmelser om sanktioner vid överträdelse av förordningen. Förslaget till dataskyddslag innehåller också en bestämmelse om tystnadsplikt för den som utsetts till dataskyddsombud enligt dataskyddsförordningen.

Samtliga dessa ovan nämnda författningsförslag avser bestämmelser av ett slag som måste finnas i svensk rätt för att Sverige ska uppfylla sina unionsrättsliga förpliktelser. Statiska hänvisningar till data-

² Prop. 2015/16:156 s. 34.

skyddsförordningen i dessa bestämmelser skulle leda till oklarheter och brister, om dataskyddsförordningen skulle komma att ändras utan att den svenska lagstiftaren hinner vidta åtgärder. Den omständigheten att somliga förändringar i dataskyddsförordningen ändå skulle kunna föranleda behov av justeringar av svensk rätt, t.ex. rörande vilken myndighet eller domstol som ska hantera en viss fråga, utgör inte skäl för att välja någonting annat än dynamiska hänvisningar i dessa paragrafer.

Vidare förekommer det i våra författningsförslag bestämmelser som föreskriver undantag från dataskyddsförordningens bestämmelser. Undantagen avser de registrerades rättigheter å ena sidan och den personuppgiftsansvariges skyldigheter å den andra. Flera av de föreslagna undantag som innehåller hänvisningar till dataskyddsförordningen är nära förknippade med den svenska grundlagsregleringen om tryck- och yttrandefrihet och rätt till tillgång till allmänna handlingar. Det råder enligt vår mening inget tvivel om att dessa undantag ska gälla, även om dataskyddsförordningens lydelse skulle komma att ändras i någon detalj. Vi föreslår även undantag som motiveras av behovet av en balans mellan det skydd som dataskyddsförordningen ger den registrerade och det skydd som annan lagstiftning ger den personuppgiftsansvariges verksamhet eller tredje parts personliga integritet, t.ex. i form av sekretess. Även i dessa bestämmelser anser vi att dynamiska hänvisningar behövs för att säkerställa att balansen består även vid en eventuell ändring av dataskyddsförordningen.

I ett fall, rörande behandling av personuppgifter utanför dataskyddsförordningens egentliga tillämpningsområde, anser vi dock att det finns skäl att välja en statisk hänvisningsteknik, innebärande att hänvisningen ska avse den ursprungliga lydelsen av dataskyddsförordningen. Skälen för detta ställningstagande utvecklas i avsnitt 6.4.2.

Det kan noteras att detta betänkande även innehåller förslag till ändringar i offentlighets- och sekretesslagen (2009:400), innebärande att hänvisningar till dataskyddsförordningen ska införas i vissa bestämmelser. Frågan om hänvisningarnas karaktär i de fallen behandlas i avsnitt 17.

5.2.3 Avvikande bestämmelser i annan lag eller i förordning ska ha företräde

Reglering av behandling av personuppgifter har i Sverige sedan lång tid tillbaka skett i form av en generell lag, kompletterad med särregler i s.k. registerförfattningar för viktigare och känsligare register. Vid införlivandet av dataskyddsdirektivet konstaterade Datalagskommittén att överväganden avseende de särskilda registerförfattningarna föll utanför deras uppdrag. Samtidigt bedömde kommittén att det även med den nya generella lagstiftningen föreföll nödvändigt att ha särregler i vissa fall. Kommittén ansåg därför att den nya lagen om behandling av personuppgifter borde innehålla en bestämmelse som innebär att särregleringen inte berörs.³ Regeringen instämde i denna bedömning.⁴ Personuppgiftslagen gjordes därför subsidiär på så sätt att om det i en annan lag eller i en förordning finns bestämmelser som avviker från lagen, ska de bestämmelserna gälla (2 § PUL).

I de fall kompletteringar till eller undantag från dataskyddsförordningen får och bör göras på generell nivå ingår det i vårt uppdrag att överväga frågan. I några fall ger emellertid förordningen utrymme för undantag eller kompletteringar avseende en särskild typ av verksamhet, se t.ex. artiklarna 9 och 23. I andra fall ges medlemsstaterna möjlighet att fastställa mer specifika villkor för att anpassa bestämmelserna i förordningen för att säkerställa en laglig och rättvis behandling, se t.ex. artikel 6.2 och 6.3 andra stycket. För att lämpliga avvägningar mellan skyddet för den personliga integriteten och behovet av att kunna behandla personuppgifter ska kunna göras i dessa situationer krävs överväganden som tar särskild hänsyn till de omständigheter som föreligger i en viss typ av verksamhet.

Det ligger inte inom ramen för vårt uppdrag att ta ställning till i vilken mån utrymmet för sektorsspecifik reglering om behandling av personuppgifter bör utnyttjas. Av kommittédirektiven framgår dock inte annat än att regeringen har för avsikt att i vart fall tills vidare hålla fast vid det traditionella systemet för reglering av behandling av personuppgifter i Sverige, dvs. i form av en generell reglering som kompletteras av sektorsspecifika författningar med bestämmelser om behandling av personuppgifter.

³ SOU 1997:39 s. 205 f.

⁴ Prop. 1997/98:44 s. 40 f.

I vissa fall kan lagform krävas enligt 2 kap. 6 och 20 §§ regeringsformen, men många gånger kan sektorsspecifika författningar som rör behandling av personuppgifter beslutas av regeringen, med stöd av dess restkompetens enligt 8 kap. 7 § första stycket 2 regeringsformen eller med stöd av bemyndiganden i lag. Det kommer följaktligen även i fortsättningen sannolikt att finnas ett stort antal förordningar som innehåller särskilda bestämmelser om behandling av personuppgifter. Bestämmelser i såväl lagar som förordningar bör därför, på motsvarande sätt som gällt hittills, ha företräde framför bestämmelserna i den generella reglering som vi föreslår. Det bör dock tydliggöras i författningstexten att dataskyddslagen är subsidiär endast i förhållande till bestämmelser om sådant som regleras i dataskyddslagen, dvs. som rör behandling av personuppgifter. Det kan t.ex. vara bestämmelser som specificerar den rättsliga grunden för en myndighets behandling av personuppgifter, begränsningar av rätten att behandla känsliga personuppgifter i en viss verksamhet eller särskilda förfaranderegler. Att denna avgränsning gällt även enligt 2 § PUL framgår av förarbetena till den bestämmelsen.⁵ Eventuella konflikter i rättstillämpningen mellan dataskyddslagens bestämmelser och sådana bestämmelser i andra författningar som avser annat än behandling av personuppgifter ska alltså lösas med hjälp av de allmänna principerna om till exempel normhierarki, EU-rättens företräde och *lex specialis*. Om en annan lag eller en förordning innehåller någon bestämmelse om behandling av personuppgifter som avviker från dataskyddslagen, ska däremot den avvikande bestämmelsen tillämpas.

Det bör betonas att den bestämmelse om subsidiaritet som vi föreslår kommer att få en betydligt mer begränsad betydelse än dess motsvarighet i 2 § PUL, även om dess innebörd är densamma. Detta beror på att dataskyddslagen, till skillnad från personuppgiftslagen, inte är heltäckande. Dataskyddslagen utgör endast ett komplement till dataskyddsförordningen och reglerar bara vissa frågor. Bestämmelsen om subsidiaritet kan bara aktualiseras i dessa fall och inte om en bestämmelse i en annan författning rörande behandling av personuppgifter avser en fråga som inte alls regleras i dataskyddslagen.

Bestämmelsen om att annan lag eller förordning ska ha företräde framför dataskyddslagen utvidgar inte heller utrymmet för att göra

⁵ Prop. 1997/98:44 s. 114 f.

nationella undantag från de direkt tillämpliga bestämmelserna i dataskyddsförordningen. Principen om unionsrättens företräde innebär att en bestämmelse i en sektorsspecifik författning får tillämpas endast om den är förenlig med dataskyddsförordningen och avser en fråga som enligt förordningen får särregleras eller specificeras genom nationell rätt.

6 Behandling av personuppgifter utanför dataskyddsförordningens tillämpningsområde

6.1 Vårt uppdrag

Dataskyddsförordningen och det nya dataskyddsdirektivet kommer sammantaget att täcka ett något större område än den nuvarande EU-rättsliga regleringen (dataskyddsdirektivet och dataskyddsrambeslutet). Utvidgningen görs främst på området som rör brottsbekämpning. Det kommer dock fortfarande att finnas ett område som inte täcks av EU-regleringen, och som inte nödvändigtvis kommer att omfattas av någon sektorsspecifik reglering. I vårt uppdrag ingår att undersöka denna fråga närmare och överväga om det finns behov av en generell reglering för sådan personuppgiftsbehandling. Enligt kommittédirektiven skulle en sådan reglering exempelvis kunna innebära att förordningen i relevanta delar görs tillämplig även utanför unionsrättens tillämpningsområde.

6.2 Gällande rätt

I artikel 3.2 första strecksatsen i dataskyddsdirektivet anges att direktivet inte gäller för sådan behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av gemenskapsrätten, exempelvis sådan verksamhet som avses i avdelningarna V och VI i fördraget om Europeiska unionen, och inte under några omständigheter behandlingar som rör allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välbefinnande när behandlingen har samband med frågor om statens säkerhet) och statens verksamhet på straffrättens område.

Personuppgiftslagen är däremot generellt tillämplig, vilket innebär att den också gäller för sådan behandling som faller utanför det nuvarande dataskyddsdirektivets tillämpningsområde. Anledningen till att denna lösning valdes var bland annat att det ansågs särskilt viktigt med ett starkt integritetsskydd för personuppgifter inom all offentlig verksamhet. Vidare ansågs den lösningen garantera att behovet av särregler i förhållande till personuppgiftslagen alltid övervägs noga i den ordning som krävs för författningsgivning.¹

Vilka verksamheter som omfattas av gemenskapsrättens tillämpningsområde framgår inte av dataskyddsdirektivet, utan följer av fördragen och EU-domstolens praxis. Artikel 3.2 första strecksatsen i dataskyddsdirektivet rörande tillämpningsområdet har kunnat tolkas som att undantagets räckvidd begränsas till den kategori av områden som nämns som exempel i bestämmelsen, det vill säga till sådan verksamhet som väsentligen omfattas av vad man brukade kalla den andra och tredje pelaren. En annan tolkning har varit att bestämmelsen undantar all verksamhet som inte omfattas av gemenskapsrätten från tillämpningsområdet för dataskyddsdirektivet.

EU-domstolen har funnit att det är den först nämnda tolkningen av bestämmelsens innebörd som gäller. Domstolen har bland annat uttalat att de verksamheter som nämns som exempel i artikel 3.2 första strecksatsen i dataskyddsdirektivet är avsedda att definiera räckvidden av det där föreskrivna undantaget, varför detta undantag endast är tillämpligt på sådan verksamhet som uttryckligen nämns där eller som kan placeras i samma kategori.²

6.3 Dataskyddsförordningen

Enligt artikel 2.2 i dataskyddsförordningen ska förordningen inte tillämpas på behandling av personuppgifter som

- a) utgör ett led i en verksamhet som inte omfattas av unionsrätten,
- b) medlemsstaterna utför när de bedriver verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken,

¹ Prop. 1997/98:44 s. 40 f.

² Dom Lindqvist, C-101/01, EU:C:2003:596, punkterna 34–35 och 44. Se även EU-domstolens tolkning av undantaget som gjordes i dom Österreichischer Rundfunk m.fl., C-465/00, C-138/01 och C-139/01, EU:C:2003:294.

- c) utförs av en fysisk person som ett led i verksamhet av privat natur eller som har samband med dennes hushåll, eller
- d) utförs av behöriga myndigheter för ändamålen att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder, inkluderande skydd mot samt förebyggande av hot mot allmän säkerhet.

I skäl 16 till dataskyddsförordningen anges verksamhet som rör nationell säkerhet som ett exempel på en verksamhet som enligt led a inte omfattas av unionsrättens tillämpningsområde. Sådan behandling av personuppgifter som avses i led d omfattas av det nya dataskyddsdirektivets tillämpningsområde.

Förordningen gäller enligt artikel 2.3 inte heller för behandling av personuppgifter som utförs av EU:s institutioner, organ och byråer. Sådan behandling regleras i stället i förordning (EG) nr 45/2001.

6.4 Överväganden och förslag

Utredningens förslag: Dataskyddsförordningen och dataskyddslagen ska i tillämpliga delar gälla även i verksamhet utanför unionsrättens tillämpningsområde och vid Sveriges deltagande i den gemensamma utrikes- och säkerhetspolitiken. Datainspektionen ska utöva tillsyn även över denna personuppgiftsbehandling.

Dataskyddsförordningen ska inte tillämpas på behandling av personuppgifter som en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll (artikel 2.2 c i dataskyddsförordningen). Inte heller ska dataskyddsförordningen tillämpas på behandling av personuppgifter som omfattas av annan unionsrättslig dataskyddsreglering, dvs. det nya dataskyddsdirektivet eller förordning (EG) nr 45/2001. Det finns emellertid behandling av personuppgifter som inte omfattas av någon unionsrättslig dataskyddsreglering överhuvudtaget, nämligen behandling som utförs antingen som ett led i en verksamhet som inte omfattas av unionsrätten, såsom verksamhet rörande nationell säkerhet, eller i en verksamhet som omfattas av den gemensamma utrikes- och

säkerhetspolitiken (dvs. leden a och b i artikel 2.2 i dataskyddsförordningen).

6.4.1 Vad faller utanför unionsrättens tillämpningsområde?

EU-domstolens tolkning av undantaget i artikel 3.2 första strecksatsen i dataskyddsdirektivet synes innebära att direktivet i vissa fall ska tillämpas trots att behandlingen av personuppgifter utgör ett led i en verksamhet som i andra sammanhang skulle anses falla utanför gemenskapsrättens tillämpningsområde. Det går inte att komma till en annan slutsats än att EU-domstolen ansett att dataskyddsdirektivet ska ha ett brett tillämpningsområde. Det finns dock fortfarande ett visst utrymme för olika tolkningar av exakt var gränserna går. Frågan är om artikel 2.2 a i dataskyddsförordningen ska tolkas på samma sätt som EU-domstolen tolkat artikel 3.2 första strecksatsen i dataskyddsdirektivet.

Syftet med dataskyddsförordningen är att säkra en enhetlig och hög skyddsnivå för fysiska personer och att undanröja hinder för flödena av personuppgifter inom unionen. Det finns ingenting i dataskyddsförordningen som antyder att unionslagstiftaren har avsett att inskränka det materiella tillämpningsområdet för dataskyddsförordningen jämfört med direktivet. Även det förhållandet att reformen syftar till att personuppgiftsbehandlingen inom unionen ska harmoniseras talar för att undantaget i artikel 2.2 a i dataskyddsförordningen inte bör ges en vidare innebörd än motsvarande bestämmelse i dataskyddsdirektivet.

Sedan dataskyddsdirektivet antogs har fördragen ändrats och innehåller numera en uttrycklig rättslig grund för antagandet av rättsakter till skydd för personuppgifter. Enligt artikel 16 i fördraget om Europeiska unionens funktionssätt har EU tilldelats befogenhet att fastställa bestämmelser om skydd för enskilda personer när det gäller behandling av personuppgifter i medlemsstaterna, när dessa utövar verksamhet som omfattas av unionsrättens tillämpningsområde, samt om den fria rörligheten för sådana uppgifter. Jämfört med vad som gällde enligt artikel 100a i fördraget om upprättandet av Europeiska gemenskapen har artikel 16 i fördraget om Europeiska unionens funk-

tionssätt utvidgat EU:s befogenheter att anta rättsakter för att skydda personuppgifter inom unionen.³

Det faktum att den nya rättsliga grunden för antagandet av unionsrättslig reglering om dataskydd uttryckligen undantar sådan verksamhet som faller utanför unionsrättens tillämpningsområde talar å andra sidan mot att tolka bestämmelsen i artikel 2.2 a i dataskyddsförordningen på samma sätt som artikel 3.2 i dataskyddsdirektivet. Därtill kommer att artikel 2.2 i förordningen har en annan utformning än artikel 3.2 i dataskyddsdirektivet. Den exemplifiering som EU-domstolen byggt sitt resonemang om vad som faller utanför gemenskapsrätten på, finns inte i förordningen. Även detta medför att det inte är självklart att bestämmelserna ska tolkas på samma sätt.

Exakt vilka verksamheter som faller utanför unionsrättens tillämpningsområde och därmed inte omfattas av förordningens bestämmelser om behandling av personuppgifter är således oklart, förutom när det gäller sådan verksamhet rörande nationell säkerhet som uttryckligen nämns i skälen. Det är dock enligt vår bedömning rimligt att anta att det inom den offentliga sektorn också finns annan verksamhet som på samma sätt som nationell säkerhet kan betraktas som en strikt nationell angelägenhet och därför faller utanför unionsrättens tillämpningsområde även vid en restriktiv tolkning av undantaget från förordningens tillämpningsområde.

6.4.2 Ska förordningens bestämmelser göras gällande utanför deras tillämpningsområde?

Frågan är då om dataskyddsförordningens bestämmelser borde gälla även vid sådan behandling av personuppgifter som enligt artikel 2.2 a och 2.2 b inte omfattas av förordningens tillämpningsområde.

Enligt vår bedömning är det sannolikt bara i den offentliga sektorn som det skulle kunna förekomma verksamhet som faller utanför unionsrättens tillämpningsområde i den mening som avses i artikel 2.2 a och där behandling av personuppgifter därmed inte skulle omfattas av dataskyddsförordningens direkt tillämpliga bestämmelser. Det är dessutom bara myndigheter och beslutande politiska för-

³ Prop. 2007/08:168 s. 52.

samlingar som deltar i den gemensamma utrikes- och säkerhetspolitiken, som avses i artikel 2.2 b.

Någon unionsrättslig allmänt gällande princip som innebär att en medlemsstat inte, med stöd av sin nationella kompetens, kan utvidga tillämpningsområdet för en EU-förordning finns inte. Det finns alltså inga formella hinder mot att utvidga tillämpningsområdet för dataskyddsförordningens bestämmelser till att omfatta även sådan personuppgiftsbehandling som faller utanför unionsrättens tillämpningsområde.⁴

När personuppgiftslagen antogs gjordes den generellt tillämplig. Anledningen till att denna lösning valdes var som ovan angetts bland annat att det ansågs särskilt viktigt med ett starkt integritetsskydd för personuppgifter inom all offentlig verksamhet. Dessa motiv är alltså aktuella.

Sverige har vidare, i enlighet med vad som anges i avsnitt 3.2 och 3.3, genom att anta bland annat Europarådets dataskyddskonvention, gjort vissa internationella åtaganden att skydda enskilda individers personliga integritet. För att säkerställa att det inom varje verksamhet finns ett fullgott skydd anser vi att förordningens bestämmelser om behandling av personuppgifter bör utsträckas till att gälla generellt. Vi anser att detta är ett bättre alternativ än att införa en komplett nationell dataskyddsreglering för verksamhet som inte omfattas av förordningens tillämpningsområde. Det skulle leda till att vissa myndigheter för sin personuppgiftsbehandling skulle tvingas tillämpa två parallella regelverk, förutom eventuellt förekommande sektorspecifika författningar. Dataskyddsförordningen bör därför, i tillämpliga delar, genom dataskyddslagen utsträckas till att gälla även vid sådan behandling av personuppgifter som enligt artikel 2.2 a och b inte omfattas av dataskyddsförordningens tillämpningsområde.

Det är inte möjligt att i nationell rätt ålägga tillsynsmyndigheter i andra länder att samarbeta med den svenska tillsynsmyndigheten. Det är därför inte möjligt att göra de bestämmelser som ålägger tillsynsmyndigheterna en skyldighet att samarbeta tillämpliga genom en bestämmelse i dataskyddslagen. Inte heller är det i nationell rätt möjligt att ge den europeiska dataskyddsstyrelsen behörighet att t.ex. utfärda riktlinjer och rekommendationer inom det område där EU inte har befogenheter i enlighet med fördragen. Det är inte heller möjligt

⁴ Jfr prop. 2010/11:80 s. 59 f.

att ge kommissionen rätt att anta delegerade akter. Kapitel VII och kapitel X i dataskyddsförordningen kan därför inte göras tillämpliga genom en reglering i dataskyddslagen. Det kan även i övrigt finnas bestämmelser i dataskyddsförordningen som inte kan tillämpas i rent nationell verksamhet. Det får därför i varje enskilt fall göras en bedömning av om förordningens bestämmelser går att tillämpa.

Sverige har inte överlåtit beslutskompetens till EU inom de områden där dataskyddsförordningens bestämmelser ska gälla enligt vårt förslag i denna del. Om förordningen ändras bör därför den svenska lagstiftaren ta ställning till om dessa ändringar ska få genomslag även på de områden som är undantagna från förordningens tillämpningsområde. Hänvisningen till förordningen i den nu aktuella bestämmelsen i dataskyddslagen bör därför vara statisk, dvs. avse den ursprungliga lydelsen av förordningen.

I avsnitt 5.2.3 har vi föreslagit att dataskyddslagen ska vara subsidiär till avvikande bestämmelser i annan lag eller i förordning. Det är således möjligt att genom sektorsspecifik författning göra undantag från den föreslagna bestämmelsen om utsträckt tillämpning av dataskyddsförordningens bestämmelser.⁵

6.4.3 Vem ska utöva tillsyn?

Utredningen om tillsynen över den personliga integriteten har föreslagit att Datainspektionen ska utses till svensk tillsynsmyndighet enligt dataskyddsförordningen och att detta ska regleras i inspektionens myndighetsinstruktion.⁶ Vi utgår i vårt betänkande från att regeringen kommer att besluta i enlighet med det förslaget. Enligt vår bedömning bör en sådan reglering, uttryckligen eller underförstått, medföra att Datainspektionen ska utöva tillsyn även i fråga om efterlevnaden av bestämmelser i nationella författningar som kompletterar dataskyddsförordningen.

Vi föreslår ovan att dataskyddsförordningens bestämmelser i tillämpliga delar ska gälla även i verksamhet utanför unionsrättens tillämpningsområde och vid Sveriges deltagande i den gemensamma utrikes- och säkerhetspolitiken. Det innebär i praktiken att data-

⁵ Jfr 1 kap. 1 § andra stycket lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.

⁶ SOU 2016:65 s. 142 f.

skyddsförordningen i dessa delar ska gälla utanför dess egentliga tillämpningsområde. Det är mot denna bakgrund inte självklart att en reglering i myndighetsinstruktionen, som i enlighet med det nämnda förslaget anger att Datainspektionen är tillsynsmyndighet enligt dataskyddsförordningen, även skulle anses omfatta tillsyn över behandling av personuppgifter som sker inom det område där förordningen fått utsträckt tillämpningsområde genom dataskyddslagen.

Enligt vår mening bör behandling av personuppgifter utanför dataskyddsförordningens egentliga tillämpningsområde stå under samma tillsyn som sådan behandling som sker med direkt tillämpning av förordningens bestämmelser. Huvudregeln bör vara att det också är samma myndighet som utövar denna tillsyn. Vi föreslår därför att det i förordningen till dataskyddslagen anges att Datainspektionen är tillsynsmyndighet enligt dataskyddslagen. Av tydlighetsskäl bör denna bestämmelse även informera om att Datainspektionen är tillsynsmyndighet enligt dataskyddsförordningen. För det fall att regeringen, under beredningen av detta betänkande och av SOU 2016:65, skulle finna att regleringen av Datainspektionens tillsynsansvar i stället ska samlas i myndighetsinstruktionen, kan den bestämmelse som vi föreslår i denna del utgå.

7 Förhållandet till yttrande- och informationsfriheten

7.1 Vårt uppdrag

Regeringen bedömer i kommittédirektiven att det genom dataskyddsförordningens artiklar 85 och 86 blir tydligare än i det nuvarande dataskyddsdirektivet att den EU-rättsliga dataskyddsregleringen inte inkräktar på området för tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Det ingår därför inte i utredningens uppdrag att överväga eller lämna förslag till grundlagsändringar. I detta sammanhang bör det noteras att det inte heller ingår i utredningens uppdrag att lämna några förslag som rör handlingsoffentligheten eller att närmare analysera innebörden av artikel 86.

Regeringen menar att det – utanför tryckfrihetsförordningens och yttrandefrihetsgrundlagens tillämpningsområde – även fortsättningsvis bör finnas behov av bestämmelser som i likhet med 7 § andra stycket PUL balanserar personuppgiftsskyddet mot yttrande- och informationsfriheten.

Vårt uppdrag är därför att analysera hur bestämmelser som balanserar personuppgiftsskyddet mot yttrande- och informationsfriheten utanför tryckfrihetsförordningens och yttrandefrihetsgrundlagens tillämpningsområde bör utformas.

7.2 Gällande rätt

Enligt artikel 9 i dataskyddsdirektivet ska medlemsstaterna besluta om undantag och avvikelser från delar av direktivet med avseende på behandling av personuppgifter som sker uteslutande för journalistiska ändamål eller konstnärligt eller litterärt skapande, om det är

nödvändigt för att förena rätten till privatlivet med reglerna om yttrandefriheten.

I 7 § första stycket PUL finns en upplysningsbestämmelse om att bestämmelserna i lagen inte ska tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Det innebär bland annat att de grundlagsskyddade rättigheterna att framställa och sprida yttranden samt meddelar- och anskaffarfriheten undantas från tillämpningsområdet.

I förarbetena gjordes den bedömningen att artikel 9 i direktivet tillåter ett hänsynstagande till bland annat konstitutionella traditioner och principer och att direktivet därför inte lägger hinder i vägen för ett generellt undantag från personuppgiftslagens bestämmelser. Regeringen uppmanade vidare till stor försiktighet vid alla ingripanden som riktar sig mot företeelser som typiskt sett åtnjuter skydd av grundlagarna. Det ansågs att även ingripanden som inte direkt strider mot någon bestämmelse, men som är oförenliga med grundlagarnas syfte, bör underlåtas.¹

Lagrådet avstyrkte bestämmelsen i 7 § första stycket med motiveringen att det fick anses tveksamt om dåvarande EG-domstolen skulle acceptera att de bestämmelser i direktivet som införlivades genom personuppgiftslagen fick vika i vidare mån än vad som framgick av ordalydelsen i direktivets artikel 9.²

I 7 § andra stycket PUL görs undantag från flertalet av lagens bestämmelser vid personuppgiftsbehandling som inte omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen men som sker uteslutande för journalistiska ändamål eller konstnärligt eller litterärt skapande. Undantaget innebär i praktiken att bara de bestämmelser i lagen som rör tillsyn och säkerhet vid behandling ska tillämpas.

Frågan om tolkningen av begreppet journalistiska ändamål har prövats i praxis både nationellt och på EU-nivå. I den så kallade Ramsbro-domen (NJA 2001 s. 409) uttalade Högsta domstolen bland annat att undantaget för journalistiska ändamål utgör ett försök att i mer generella termer ge uttryck för en intresseavvägning mellan intresset av skydd för privatlivet och intresset av yttrandefrihet. Att

¹ Prop. 1997/98:44 s. 50 f.

² Prop. 1997/98:44 s. 236 f.

uttrycket journalistiska ändamål använts kan enligt domstolen under sådana förhållanden inte antas vara i avsikt att privilegiera etablerade massmedier eller personer som är yrkesverksamma inom sådana medier, utan får antas vara avsett att betona vikten av en fri informations-spridning i frågor av betydelse för allmänheten eller för grupper av människor och en fri debatt i samhällsfrågor. Ramsbro-domen har i doktrinen ansetts visa att en betydande del av det som sker på internet omfattas av undantaget i 7 § andra stycket PUL.³

I domen i det så kallade Satakunnan-målet⁴ uttalade EU-domstolen att de begrepp som hör samman med yttrandefriheten, däribland journalistik, måste tolkas vitt. Domstolen fann därför att den verksamhet som företaget Satakunnan bedrev – dvs. att uppgifter om fysiska personers inkomster och förmögenheter samlades in från offentliga källor, sorterades, publicerades i tryck och distribuerades via en sms-tjänst – skulle anses ske uteslutande för journalistiska ändamål om verksamheten endast syftade till att sprida information, åsikter eller idéer till allmänheten. EU-domstolen uttalade vidare att sådan verksamhet inte bara skulle anses förbehållen medieföretag. EU-domstolen överlät dock till den nationella domstolen att avgöra om det i just Satakunnan-fallet var fråga om en verksamhet som endast syftade till att sprida information till allmänheten. Den finska Högsta förvaltningsdomstolen ansåg att så inte var fallet (23.9.2009/2303 HFD 2009:82).⁵

Undantaget för journalistiska ändamål är alltså inte begränsat till journalister eller traditionella massmedier. Även en privatperson kan anses behandla personuppgifter för sådana ändamål, t.ex. på en blogg, förutsatt att uppgifterna inte är av rent privat karaktär.

³ Öman och Lindblom, Personuppgiftslagen, (20 december 2016, Zeteo), kommentaren till 7 § PUL. Svahn Starrsjö, Personuppgiftslagen och yttrandefriheten, SvJT 100 år (jubileumsskrift) s. 447.

⁴ Dom Satakunnan Markkinapörssi Oy och Satamedia Oy, C-73/07, EU:C:2008:727.

⁵ Saken är dock fortfarande föremål för prövning, nu i Europadomstolen, Satakunnan Markkinapörssi OY och Satamedia OY v. Finland, nr 931/13, dom den 21 juli 2015, hänskjuten till Grand Chamber den 14 december 2015.

7.3 Dataskyddsförordningen

Enligt artikel 85.1 i dataskyddsförordningen ska medlemsstaternas nationella lagstiftning förena rätten till skydd av personuppgifter i enlighet med förordningen med rätten till yttrande- och informationsfrihet, inbegripet personuppgiftsbehandling för journalistiska ändamål samt för akademiskt, konstnärligt eller litterärt skapande. När det gäller behandling för sådana ändamål ska medlemsstaterna enligt artikel 85.2 föreskriva om undantag eller avvikelser från i artikeln angivna delar av förordningens bestämmelser om det behövs för att förena rätten till skydd för personuppgifter med yttrande- och informationsfriheten. Medlemsstaterna ska enligt artikel 85.3 underätta kommissionen om de undantagsbestämmelser som de har antagit med stöd av artikel 85.2.

I skäl 153 anges att behandling av personuppgifter endast för journalistiska, akademiska, konstnärliga eller litterära ändamål bör undantas från viss tillämpning för att förena rätten till skydd för personuppgifter med rätten till yttrande- och informationsfrihet som följer av artikel 11 i EU:s stadga om de grundläggande rättigheterna. Av nämnda artikel i stadgan framgår att var och en har rätt till yttrandefrihet, att denna rätt innefattar åsiktsfrihet samt frihet att ta emot och sprida uppgifter och tankar utan offentlig myndighets inblandning och oberoende av territoriella gränser. Artikel 11 slår också fast att mediernas frihet och mångfald ska respekteras.

I förordningens skäl 153 anges också att medlemsstaterna bör anta lagstiftningsåtgärder som fastställer de olika undantag som behövs för att balansera de två grundläggande rättigheterna, samt att det bör göras en bred tolkning av vad som innefattas i yttrandefriheten.

7.4 Våra överväganden och förslag

Utredningens förslag: En upplysningsbestämmelse som tydliggör att bestämmelserna i dataskyddslagen och dataskyddsförordningen inte ska tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen, ska tas in i dataskyddslagen.

Ett undantag för sådan behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande ska också införas. Dataskyddsförordningens bestämmelser om syfte, tillämpningsområde och definitioner samt bestämmelser om säkerhet för personuppgifter, tillsyn, rättsmedel, ansvar och sanktioner ska dock tillämpas även i dessa fall.

Något om vårt uppdrag

Våra detaljerade tryck- och yttrandefrihetsgrundlagar är unika i jämförelse med hur motsvarande reglering ser ut i övriga Europa. Relationen såväl mellan EU-rätten och de svenska tryck- och yttrandefrihetsgrundlagarna, som mellan tryck- och yttrandefrihetsgrundlagarna och den personliga integriteten, har varit föremål för debatt och en rad utredningar på senare år.⁶ För en nyligen genomförd genomgång av EU-rättens förhållande till grundlagsregleringen om tryck- och yttrandefrihet hänvisas till Mediegrundlagskommitténs betänkande SOU 2016:58, avsnitt 5.4 och 14.1.

I vår utrednings uppdrag ingår inte att närmare analysera förhållandet mellan grundlagsskyddet för informations- och yttrandefriheten och rätten till skydd av personuppgifter enligt dataskyddsförordningen. Följaktligen är det inte heller vår uppgift att föreslå bestämmelser som påverkar balansen mellan dessa grundläggande fri- och rättigheter, exempelvis förändrade förutsättningar för journalister, bloggare och innehavare av utgivningsbevis att behandla personuppgifter.

Vårt uppdrag är i stället att analysera hur vi i svensk rätt ska genomföra skyldigheten i förordningens artikel 85 att förena rätten till integritet med yttrande- och informationsfriheten, utan att i sak förändra möjligheterna till behandling av personuppgifter. Uppdraget är begränsat till hur en reglering som balanserar personuppgiftsskyddet mot yttrande- och informationsfriheten *utanför* tryckfrihetsförordningens och yttrandefrihetsgrundlagens tillämpningsområde

⁶ Tryck- och yttrandefrihetsberedningen i SOU 2006:96, Yttrandefrihetskommittén i SOU 2012:55 och Mediegrundlagskommittén i SOU 2016:58. Se även Integritet och straffskydd, SOU 2016:7. Debatt har förts i SvJT på senare tid; se Olle Abrahamsson och Henrik Jermsten i SvJT 2014, s. 201 och 2015, s. 8, Göran Lambertz i SvJT 2014, s. 440 samt Magnus Schmauch i SvJT 2014, s. 520 och 2015, s. 199.

bör utformas, dvs. en reglering som motsvarar den i 7 § andra stycket PUL.

Utgångspunkter för utredningens överväganden

Som framgår ovan är en utgångspunkt att vi ska undvika att föreslå förändringar i sak när det gäller förutsättningar för personuppgiftsbehandling på det här aktuella området.

Regleringen i förordningen ligger i sak nära den som finns i dataskyddsdirektivet. Förordningens reglering av förhållandet till yttrande- och informationsfriheten innebär inte några inskränkningar utan ger till sin ordalydelse ett något större utrymme för undantag än direktivet, bland annat på det sättet att det inte längre föreskrivs att behandling ska ske ”uteslutande” för journalistiska ändamål för att undantag ska kunna göras. Undantaget i artikel 85.2 har också fått ett vidare tillämpningsområde genom att akademiskt skapande lagts till. Dessutom uttalas i skäl 153 att begreppet yttrandefrihet ska ges en bred tolkning. I doktrinen har artikel 85 ansetts ge ett relativt stort utrymme för medlemsstaterna att själva välja hur regleringen utformas.⁷

Mot denna bakgrund är vår bedömning att den reglering vi föreslår kan och bör utformas med den befintliga regleringen i 7 § PUL som förebild.

Behovet av en upplysningsbestämmelse

Som framgår av kommittédirektiven har vi inte i uppdrag att föreslå någon författningsreglering som rör förordningens förhållande till behandling som sker i verksamhet som omfattas av tillämpningsområdet för tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Vi anser dock att det är angeläget att dataskyddsförordningens och dataskyddslagens bestämmelser inte ger upphov till osäkerhet kring möjligheterna till personuppgiftsbehandling på det grundlagsreglerade området, eftersom det kan påverka vitala och mycket känsliga delar av opinionsskapande verksamhet, såsom meddelarfrihet och

⁷ Wagner och Benecke, National Legislation within the Framework of the GDPR, European Data Protection Law Review 3/2016, s. 356.

källskydd. Det faktum att vi nu har att göra med en direkt tillämplig förordning, där överträdelser kan leda till kännbara sanktionsavgifter, gör det än mer angeläget att regleringen av den grundlagsskyddade verksamheten är så tydlig som möjligt när det gäller förhållandet till tryckfrihetsförordningen och yttrandefrihetsgrundlagen.

Den befintliga upplysningsbestämmelsen i 7 § första stycket PUL bedömdes av riksdag och regering som förenlig med dataskyddsdirektivets likartade bestämmelser vid införandet av personuppgiftslagen.⁸ Den har inte varit föremål för domstolsprövning och heller inte ifrågasatts av kommissionen sedan införandet för snart tjugo år sedan. Eftersom förordningen, som nämnts ovan, tycks ge ett ökat utrymme för undantag med hänsyn till yttrande- och informationsfriheten bedömer vi att förordningen inte hindrar att en upplysningsbestämmelse motsvarande den i 7 § första stycket PUL införs i dataskyddslagen.

Undantag för journalistiska ändamål m.m.

Ordalydelsen i förordningens artikel 85.2 synes ålägga medlemsstaterna att göra vissa undantag från förordningen för behandling som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande. Undantag får dock bara göras om de är nödvändiga för att förena rätten till integritet med yttrande- och informationsfriheten. Samma krav på nödvändighet finns i direktivet, och den befintliga bestämmelsen i 7 § andra stycket PUL bedömdes vara nödvändig för att personuppgiftslagens bestämmelser skulle vara förenliga med yttrande- och informationsfriheten.

Begreppet akademiskt skapande är nytt och definieras inte närmare i skäl eller artikeltext. Vår bedömning är att det knappast torde vara att likställa med forskning, eftersom forskning är särreglerad på annat sätt i förordningen, exempelvis i artikel 9.2 j och artikel 89. Möjligen skulle behandling i samband med själva färdigställandet och spridningen av texter med vetenskapligt innehåll kunna avses. Innebörden av begreppet är dock oklar och dess närmare betydelse får utvecklas i praxis.

⁸ Prop. 1997/98 44 s. 48 f., bet. 1997/98:KU18, rskr.1997/98:180.

Undantagsbestämmelsen i 7 § andra stycket PUL har bland annat ansetts tillämplig på journalistisk verksamhet på internet som resulterar i yttranden som bara sprids där och för kommunikation som inte bedrivs av yrkesverksamma journalister.⁹ Betydelsen av opinionsbildande genom alternativa kanaler såsom sociala medier, bloggar och liknande har ökat dramatiskt under senare år, vilket innebär att skälen för ett sådant undantag i vart fall inte har minskat. Det ska noteras att viss användning av sociala medier omfattas av det så kallade privatundantaget, dvs. artikel 2.1 c i dataskyddsförordningen.¹⁰

Förordningens artikel 85.2 möjliggör undantag från förordningen i stort sett i samma utsträckning som dataskyddsdirektivet gör. De delar av förordningen som inte räknas upp i artikel 85.2, från vilka undantag alltså inte får göras, är kapitel I om tillämpningsområde och definitioner, kapitel VIII om rättsmedel, ansvar och sanktioner samt kapitel X och XI som innehåller genomförande- och slutbestämmelser. I linje med de utgångspunkter vi redogjort för ovan menar vi att det är lämpligt att utnyttja möjligheterna till undantag från förordningen i väsentligen samma utsträckning som personuppgiftslagen har undantagits i dag. Vi anser därför att undantag från bestämmelserna i dataskyddslagen och dataskyddsförordningen bör göras så långt förordningen medger, med undantag för de bestämmelser som rör säkerhet för personuppgifter och tillsyn.

Detta innebär enligt vår bedömning att bestämmelserna i förordningens kapitel II och III, artiklarna 24–30 och 35–43 och kapitel V i dataskyddsförordningen bör undantas från tillämpning, liksom de delar av dataskyddslagen som har stöd i de bestämmelserna. Kapitel IX (bestämmelser om särskilda behandlingssituationer) bedömer vi knappast blir tillämpligt för den behandling som avses här, varför det inte uttryckligen behöver undantas. Detsamma gäller kapitel X (delegerade akter och genomförandeakter) och kapitel XI (slutbestämmelser).

⁹ Prop. 1997/98:44 s. 52 f. och NJA 2001 s. 409.

¹⁰ I skäl 18 i dataskyddsförordningen görs vissa uttalanden om privat verksamhet och sociala medier.

8 Rättslig grund för behandling av personuppgifter

8.1 Vårt uppdrag

Enligt artikel 6.3 första stycket i dataskyddsförordningen ska den grund för behandlingen som avses i artikel 6.1 c och e fastställas i enlighet med unionsrätten eller den nationella rätten. Enligt kommittédirektiven innebär detta att det inte kommer att vara möjligt att endast stödja sig på den generella regleringen i förordningen vid sådan behandling. Vi har därför fått i uppdrag att analysera vad dataskyddsförordningens krav i denna del innebär i fråga om nationell författningsreglering och om det bör införas generella bestämmelser till stöd för åtminstone den offentliga sektorns behandling av personuppgifter. Informationshanteringsutredningens förslag till 8 § myndighetsdatalag¹, med beaktande av de synpunkter som framförts vid remissbehandlingen, är enligt kommittédirektiven en lämplig utgångspunkt.

8.2 Dataskyddsförordningen

8.2.1 Laglig behandling

Den europeiska dataskyddsregleringen utgår från att varje behandling av personuppgifter måste vila på en rättslig grund. Behandling av personuppgifter får därför bara ske under de omständigheter som särskilt anges i lagstiftningen. I dataskyddsförordningen räknas dessa rättsliga grunder upp i artikel 6.1. Behandling är enligt denna bestämmelse endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:

¹ SOU 2015:39.

- a) Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.
- b) Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.
- c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.
- d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.
- e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.
- f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

Artikel 6.1 i dataskyddsförordningen motsvarar i stora drag artikel 7 i dataskyddsdirektivet, som har genomförts i svensk rätt genom 10 § PUL. Den största skillnaden är att det enligt förordningen inte är tillåtet för myndigheter att, när de fullgör sina uppgifter, behandla personuppgifter med stöd av den rättsliga grund som utgår från en avvägning mellan den ansvariges berättigade intressen och den registrerades rättigheter och intressen (jfr 10 § f PUL). Den möjligheten kvarstår däremot för privata aktörer som behandlar personuppgifter. I andra stycket av artikel 6.1 anges nämligen att led f i första stycket inte ska gälla för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter.

Uppräkningen i artikel 6.1 är uttömmande. Om inget av dessa villkor är uppfyllda är behandlingen inte laglig och får därmed inte utföras. De olika villkoren är i viss mån överlappande. Flera rättsliga grunder kan därför vara tillämpliga avseende en och samma behandling.

Den omständigheten att behandlingen är laglig enligt artikel 6.1 i dataskyddsförordningen, dvs. att den är rättsligt grundad, innebär

inte att behandling kan ske av vilka uppgifter som helst eller på valfritt sätt. Den personuppgiftsansvarige måste också uppfylla kraven i övriga bestämmelser i förordningen, t.ex. de allmänna principerna i artikel 5. I artiklarna 7 och 8 anges närmare villkor för tillämpningen av artikel 6.1 a, dvs. den rättsliga grund som utgörs av den registrerades samtycke, se avsnitt 9 avseende barns samtycke. När det gäller behandling som avser särskilda kategorier av personuppgifter (känsliga personuppgifter) eller personuppgifter som rör lagöverträdelse anges ytterligare villkor i artiklarna 9 och 10, utöver dem som anges i artikel 6.1, se närmare avsnitt 10 och 11.

Enligt artikel 6.2 i förordningen får medlemsstaterna behålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen med hänsyn till behandling av personuppgifter för att efterleva artiklarna 6.1 c och 6.1 e. Denna typ av mer specifika nationella bestämmelser förekommer ofta i svenska registerförfattningar och kommer framför allt att utgöra en precisering av de allmänna principer för behandlingen som anges i artikel 5 i dataskyddsförordningen.

8.2.2 Begreppet nödvändig

För att en behandling av personuppgifter ska vara tillåten enligt artikel 6.1 b–f måste den vara nödvändig för att fullgöra, skydda eller utföra den rättsliga grunden. Enligt Svenska Akademiens Ordbok betyder det svenska ordet nödvändig att någonting absolut fordras eller inte kan underlåtas. Det unionsrättsliga begreppet har dock inte riktigt denna strikta innebörd. Nödvändighetsrekvisitet i artikel 7 i dataskyddsdirektivet har inte ansetts utgöra ett krav på att det ska vara omöjligt att fullgöra förpliktelsen eller utföra uppgiften utan att behandlingsåtgärden vidtas.² Den slutsatsen får stöd av EU-domstolens dom i målet Huber mot Tyskland, som rörde tolkningen av motsvarande nödvändighetsrekvisit i artikel 7 e i direktivet.³ EU-domstolen uttalade att en myndighets förande av ett centralt register över uppgifter som redan fanns i regionala register är nödvändigt om det bidrar till att effektivisera tillämpningen av relevanta bestämmel-

² SOU 1997:39 s. 361 f.

³ Dom Huber mot Tyskland, C-524/06, EU:C:2008:724.

ser. Domen bör kunna utgöra stöd även vid tolkningen av den nya förordningen. Även om exempelvis en uppgift av allmänt intresse skulle kunna utföras utan att personuppgifter behandlas på visst sätt, kan behandlingen anses vara nödvändig och därmed tillåten enligt artikel 6, om behandlingen leder till effektivitetsvinster. Det bör noteras att rekvisitet nödvändig inte ska förväxlas med rekvisitet absolut nödvändig, som används i andra sammanhang än rörande rättslig grund, se avsnitt 10.6.2.

8.2.3 Förhållandet mellan artiklarna 5 och 6 i dataskyddsförordningen

Utöver det grundläggande kravet på att all behandling måste vara laglig, i betydelsen att någon av de rättsliga grunder som anges i artikel 6.1 i dataskyddsförordningen är uppfylld, omgärdas varje behandling av personuppgifter av mer specifika krav. Principerna för behandling av personuppgifter, dvs. vilka allmänna krav som gäller för all personuppgiftsbehandling, anges i artikel 5.1 i dataskyddsförordningen. Artikel 5.1 i dataskyddsförordningen motsvarar i stora drag artikel 6 i dataskyddsdirektivet, som har genomförts i svensk rätt genom 9 § PUL.

Den första principen som läggs fast i artikel 5.1 (led a) är att personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Principen om laglighet utgör en hänvisning till de rättsliga grunderna i artikel 6.1. Såvitt avser principen om korrekthet kan det vid en jämförelse med andra språkversioner ifrågasättas om den svenska termen korrekt motsvarar avsikten med bestämmelsen. I den danska språkversionen anges i stället att uppgifterna ska behandlas *rimeligt*. På motsvarande sätt används i den engelska språkversionen termen *fairly*, vilket betyder rättvist, skäligt eller rimligt. I den franska språkversionen används termen *loyale*, vilken har motsvarande betydelse som engelskans *fairly*. I den tyska språkversionen används uttrycket *Treu und Glauben*, vilket brukar översättas med god tro eller tro och heder. Alla dessa termer indikerar enligt vår mening, tydligare än den svenska termen korrekt, att en intresseavvägning ska göras. I det enskilda fallet kan det således till exempel vara oförenligt med principen om ”korrekthet” att vidta en viss behandlingsåtgärd, även om denna i och

för sig skulle kunna anses vara rättsligt grundad enligt artikel 6, nämligen om behandlingen är oskälig i förhållande till den registrerade.

I artikel 5.1 anges vidare att personuppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och att de inte senare får behandlas på ett sätt som är oförenligt med dessa ändamål (led b). Principen om att ändamålen ska vara berättigade utgör i likhet med principen om laglighet en direkt koppling till de rättsliga grunderna i artikel 6.1. Ett ändamål som inte är berättigat i förhållande till den tillämpliga rättsliga grunden är således inte förenligt med artikel 5. Kravet på att ändamålen ska vara berättigade går dock längre än så och omfattar även ett krav på förenlighet med till exempel konstitutionella och andra rättsliga principer. Vidare kan även det allmänna sammanhanget och omständigheterna i det aktuella ärendet vara av betydelse för bedömningen av om ändamålen är berättigade.⁴ Ett tydligt angivet ändamål är för övrigt som regel en förutsättning för att man ska kunna bedöma om en viss behandling är laglig, dvs. om den är nödvändig i något av de sammanhang som räknas upp i artikel 6.1 b–f.

Kopplingen mellan den rättsliga grunden och kravet på särskilda, uttryckligt angivna och berättigade ändamål förstärks genom data-skyddsförordningen, där det i artikel 6.3 andra stycket anges att syftet med behandlingen (*the purpose of the processing*) i fråga om behandling som grundar sig på en rättslig förpliktelse ska framgå av förpliktelsen. Vad gäller myndighetsutövning och uppgifter av allmänt intresse anges i stället att ändamålet med behandlingen ska vara nödvändigt för att utföra uppgiften eller myndighetsutövningen.

Vidare ska uppgifterna enligt artikel 5.1 bland annat vara adekvata och korrekta (*accurate*) och får inte förvaras under en längre tid än vad som är nödvändigt (leden c, d och e). Uppgifterna måste också behandlas på ett sätt som säkerställer lämplig säkerhet (led f).

Förordningen ställer inte något krav på att de särskilda ändamålen ska vara fastställda i författning, men det finns heller ingenting som hindrar att detta görs, förutsatt att bestämmelserna uppfyller ett mål av allmänt intresse och är proportionella mot det legitima mål som eftersträvas (artikel 6.3 andra stycket). Oavsett om ändamålen fastställts i författning eller inte är det dock alltid den personuppgifts-

⁴ Artikel 29-gruppens yttrande 3/2013 om ändamålsbegränsning, s. 11–12 och 19–20.

ansvarige som ansvarar för, och ska kunna visa att, principerna i artikel 5 efterlevs (artikel 5.2).

Artiklarna 5 och 6 i dataskyddsförordningen är grundläggande och kumulativa. Dels måste någon av de rättsliga grunder som anges i artikel 6.1 vara tillämplig, dels måste samtliga principer i artikel 5.1 följas. Det är endast om någon av de rättsliga grunder som anges i artikel 6.1 är tillämplig som behandling av personuppgifter över huvud taget får ske. Om behandlingen är laglig enligt artikel 6 ska kraven i artikel 5 uppfyllas. I det följande behandlas enbart artikel 6.

8.3 Överväganden och förslag

8.3.1 Grunden för behandlingen ska i vissa fall vara fastställd

Utredningens bedömning: Artikel 6.1 c och e i dataskyddsförordningen är direkt tillämpliga. Kravet i artikel 6.3 första stycket på att grunden för behandlingen ska vara fastställd i enlighet med unionsrätten eller den nationella rätten utgör ett ytterligare villkor för tillämpning som ska vara uppfyllt. Med grunden för behandlingen avses den rättsliga förpliktelsen, uppgiften av allmänt intresse respektive myndighetsutövningen. Som en följd av den svenska arbetsmarknadsmodellen kan rättsliga förpliktelser och uppgifter av allmänt intresse vara fastställda genom kollektivavtal.

Vad är grunden för behandlingen?

I artikel 6.3 i dataskyddsförordningen första stycket anges att den grund för behandlingen som avses i punkt 1 c och e ska fastställas i enlighet med a) unionsrätten, eller b) en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av.⁵

Det står klart att den grund för behandlingen som avses i artikel 6.1 a är samtycket och att avtalet är den grund för behandlingen som avses i led b. På motsvarande sätt måste uttrycket ”den grund för behandlingen som avses i punkt 1 c och e” avse den rättsliga förpliktelsen respektive uppgiften av allmänt intresse eller rätten att utöva myndighet. Denna tolkning överensstämmer med Europeiska datatillsynsmannens förslag till förtydligande av bestämmelsen. Han har, bland annat i ett yttrande den 28 juli 2015, rekommenderat att uttrycket *The basis for the processing referred to in point (c) and (e) of paragraph 1* skulle ersättas med *The legal obligation, task, or official authority referred to in points (c) and (e) of paragraph 1*.⁶

Med grunden för behandlingen kan enligt vår mening inte avses behandlingen i sig. Om själva behandlingen ska fastställas skulle nämligen t.ex. myndighetsutövning inte kunna ske och uppgifter av allmänt intresse inte kunna utföras, om det inte utöver den lag som fastställer befogenheten också uttryckligen reglerades att behandling av personuppgifter får ske. En sådan tolkning av begreppet grunden för behandlingen skulle leda till ett närmast oöverskådligt regleringsbehov, inte minst i de många medlemsstater som inte har den tradition av sektorspecifika registerförfattningar som Sverige har. Detta kan rimligen inte ha varit avsikten, i synnerhet med tanke på dataskyddsreformens harmoniseringssyfte. Det bör också noteras att det i artikel 6.3 inte anges att ”behandlingen” ska fastställas, utan att grunden för behandlingen ska fastställas.

⁵ I den engelska versionen av artikel 6.3 första stycket i dataskyddsförordningen anges följande. *The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by: (a) Union law; or (b) Member State law to which the controller is subject.* I den franska versionen anges följande. *Le fondement du traitement visé au paragraphe 1, point c) et e), est défini par: a) le droit de l'Union; ou b) le droit de l'État membre auquel le responsable du traitement est soumis.* I kommissionens ursprungliga förslag angavs att grunden för behandlingen *must be provided for*, i stället för *shall be laid down by*. Europaparlamentet drev länge ståndpunkten att detta borde bytas ut mot *must be established in accordance with*. Under trepartsdialogen enades parterna om att använda uttrycket *shall be laid down by* (rådets dokument nr 13884/15, s. 2). Det anslutande skäl 45 kompletterades därefter på ordförandeskapets initiativ (rådets dokument 14318/15 s. 5).

⁶ Bilaga till Europeiska datatillsynsmannens yttrande 3/2015 s. 31.

EU-förordningar är direkt tillämpliga i medlemsstaterna och ska till skillnad från direktiv inte genomföras genom nationella författningsåtgärder. Att grunden för behandlingen ska fastställas kan därför inte heller innebära att de villkor som anges i artikel 6.1 c och e ska upprepas i nationell rätt.

Ett av syftena bakom kravet på fastställande i artikel 6.3 första stycket i dataskyddsförordningen har antagits vara att tydliggöra att den personuppgiftsansvarige inte får finna en rättslig grund för behandling av personuppgifter i tredje lands lagstiftning.⁷ Bestämmelsen innebär nämligen att en rättslig förpliktelse som följer av tredje lands lagstiftning inte utgör en rättslig grund för behandling av personuppgifter, även om behandlingen är nödvändig för att uppfylla förpliktelsen. På motsvarande sätt utgör det ingen rättslig grund för behandling av personuppgifter att en uppgift av allmänt intresse är fastställd i tredje lands lagstiftning.

Begränsningen till unionsrätten och medlemsstaternas nationella rätt torde främst vara av relevans för dels de personuppgiftsansvariga som har verksamhetsställen både inom och utom unionen, dels de som inte är etablerade i unionen men som har anledning att behandla personuppgifter avseende registrerade som befinner sig i unionen (artikel 3). Skälet till att det uttryckligen hänvisas till unionsrätten och medlemsstaternas nationella rätt kan förmodas vara att förordningens territoriella tillämpningsområde är vidare än det som gäller enligt dataskyddsdirektivets ordalydelse. Direktivet gäller nämligen inte för behandling av personuppgifter när den personuppgiftsansvarige inte är etablerad inom unionen, annat än om denne använder utrustning som befinner sig inom unionens territorium. Direktivet gäller inte heller om sådan utrustning används endast för att låta uppgifter passera genom gemenskapen (artikel 4.1 c). Några sådana begränsningar avseende tillämpningsområdet finns inte i dataskyddsförordningen, som i stället gäller all behandling som avser registrerade som befinner sig i unionen, om behandlingen har anknytning till utbudande av varor eller tjänster till sådana registrerade i unionen eller övervakning av deras beteende så länge beteendet sker inom unionen (artikel 3.2).

⁷ D-post: BRYR/2016-05-01/1503.

Vad menas med att grunden ska vara fastställd?

Artikel 6.3 första stycket i dataskyddsförordningen innehåller ett uttryckligt krav på att grunden för behandlingen ska vara fastställd i enlighet med unionsrätten eller den nationella rätten. Något motsvarande krav finns inte i dataskyddsdirektivet. Det är därför möjligt att med stöd av 10 § d PUL utföra behandling av personuppgifter som är nödvändig för att utföra en arbetsuppgift av allmänt intresse, även om uppgiften inte är fastställd i författning eller liknande. Viss ledning för förståelsen av artikel 6.3 kan möjligen hämtas från förordningens ingress. I skäl 45 anges bland annat att dataskyddsförordningen inte medför något krav på en särskild lag för varje enskild behandling, utan att det kan räcka med en lag som grund för flera behandlingar som bygger på en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller om behandlingen krävs för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning.

I skäl 47 anges bland annat följande, apropå att den rättsliga grund som bygger på en intresseavvägning (artikel 6.1 f) inte är tillämplig för myndigheter när de fullgör sina uppgifter.

Med tanke på att det är lagstiftarens sak att genom lagstiftning tillhandahålla den rättsliga grunden för de offentliga myndigheternas behandling av personuppgifter, bör den rättsliga grunden inte gälla den behandling de utför som ett led i fullgörandet av sina uppgifter.

Enligt vår bedömning innebär kravet på att grunden för behandlingen ska fastställas inte att det krävs en särskild reglering med anledning av dataskyddsförordningens ikraftträdande. Förekomsten av reglering avgör dock i vilken utsträckning personuppgiftsansvariga kan åberopa de rättsliga grunder som avses i leden c och e. Kravet på att grunden för behandlingen ska vara fastställd i enlighet med unionsrätten eller den nationella rätten utgör således ett villkor som måste vara uppfyllt för att bestämmelserna i artikel 6.1 c och e ska vara tillämpliga. Förpliktelser, uppgifter av allmänt intresse och myndighetsutövning som inte är rättsligt förankrade i enlighet med unionsrätten eller medlemsstatens nationella rätt kan därmed inte åberopas som rättsliga grunder för behandling av personuppgifter.

Innebörden av artikel 6.1 c är därmed att behandling av personuppgifter är laglig om behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som är fastställd i enlighet med unionsrätten eller den nationella rätten och som åvilar den personuppgiftsansvarige. På

motsvarande sätt är innebörden av artikel 6.1 e att behandling av personuppgifter är laglig om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse som är fastställd i enlighet med unionsrätten eller den nationella rätten eller om behandlingen är nödvändig som ett led i den personuppgiftsansvariges myndighetsutövning som är fastställd i enlighet med unionsrätten eller den nationella rätten.

Vilket slags reglering avses?

Grunden för behandlingen ska enligt artikel 6.3 första stycket i data-skyddsförordningen fastställas i enlighet med unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av. Med detta avses inte att den rättsliga grunden nödvändigtvis måste fastställas i eller i enlighet med en av riksdagen beslutad lag. Däremot måste grunden vara fastställd i laga ordning, på ett konstitutionellt korrekt sätt. Av skäl 41 till förordningen framgår att den rättsliga grunden bör vara tydlig och precis och dess tillämpning förutsägbar för dem som omfattas av den, i enlighet med rättspraxis vid Europeiska unionens domstol och Europeiska domstolen för de mänskliga rättigheterna. Huruvida de rättsliga förpliktelser, de uppgifter av allmänt intresse och den myndighetsutövning som har fastställts i enlighet med svensk rätt är tillräckligt precisa måste bedömas från fall till fall i rättstillämpningen.

Kollektivavtal

Den svenska arbetsmarknadsmodellen innebär att arbetsmarknadens parter i stor utsträckning reglerar arbets- och anställningsvillkor genom kollektivavtal. Kollektivavtalen innehåller en rad bestämmelser som arbetsmarknadens parter och medlemmarna i de avtalslutande organisationerna är skyldiga att följa, t.ex. om föräldratillägg, semesterlön, övertidsersättning och ersättning för läkarbesök och läkemedel. Överträdelse av bestämmelserna kan föranleda skadeståndsansvar. Avtalen har även betydelse för tredje man eftersom de ska tillämpas på samma sätt i förhållande till alla arbetstagare och således även i förhållande till oorganiserade arbetstagare och arbets-

tagare som är medlemmar i en annan arbetstagarorganisation än den som avtalet slutits med.

Reglering i kollektivavtal har i Europadomstolens praxis ansetts i sig förenlig med kravet enligt Europakonventionen att åtgärder med rättighetsbegränsande effekter ska ha stöd i lag. En bedömning får ske i det enskilda fallet med beaktande av de krav på bland annat proportionalitet som gäller vid lagstiftning eller andra åtgärder som inskränker enskildas rättigheter enligt Europakonventionen.⁸ Denna praxis talar för att samma princip bör gälla vid tillämpningen av EU-lagstiftning som rör fri- och rättigheter, såsom dataskyddsförordningen. Grunden för behandlingen av personuppgifter, även avseende oorganiserade arbetstagare, bör därför i princip kunna anses vara fastställd i enlighet med svensk rätt om den fastställts genom kollektivavtal.

8.3.2 Behandling för att uppfylla en rättslig förpliktelse

Utredningens förslag: Det ska tydliggöras att personuppgifter får behandlas om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som gäller enligt lag eller annan författning eller som följer av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning.

Begreppet rättslig förpliktelse

Bestämmelsen i artikel 6.1 c i dataskyddsförordningen är i sak likalydande med artikel 7 c i dataskyddsdirektivet – personuppgifter får behandlas om behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Begreppet rättslig förpliktelse i de båda rättsakterna bör tolkas och tillämpas på samma sätt.

För att en skyldighet ska utgöra en ”rättslig” förpliktelse måste den ha en legal grund. Detta följer både av begreppet i sig och av kra-

⁸ Jfr Europadomstolens dom i målet *Evaldsson mot Sverige*, nr 75252/01, dom den 13 februari 2007.

vet i artikel 6.3 första stycket i dataskyddsförordningen om att grunden för behandlingen ska fastställas i enlighet med unionsrätten eller den nationella rätten. Detta innebär inte att förpliktelsen nödvändigtvis måste framgå av en författning eller liknande. Rättsliga förpliktelser kan också framgå av exempelvis förelägganden, myndighetsbeslut och domar som har meddelats med stöd av gällande rätt.

Rent språkligt omfattar begreppet rättslig förpliktelse även sådana skyldigheter som har lagts fast i någon annan av rättsordningen erkänd ordning, t.ex. i ett avtal. Som en följd av den svenska arbetsmarknadsmodellen kan således rättsliga förpliktelser följa av kollektivavtal, se avsnitt 8.3.1. Förpliktelser som följer av avtal där den registrerade själv är part utgör däremot en separat rättslig grund för personuppgiftsbehandling enligt både dataskyddsdirektivet och dataskyddsförordningen, nämligen led b i respektive artikel. De rättsliga förpliktelser som avses i led c bör därmed vara av ett annat slag. I första hand leds tanken till offentligrättsliga förpliktelser. Det finns dock även i civilrättsliga författningar bestämmelser som i sig utgör eller kan medföra rättsliga skyldigheter, t.ex. inom arbetsrätten.⁹

Syftet med behandlingen ska framgå av förpliktelsen

Enligt artikel 6.3 andra stycket första meningen i dataskyddsförordningen ska syftet med behandlingen (*the purpose of the processing*) fastställas i (*be determined in*) den rättsliga grunden. Den rättsliga grunden i fråga om behandling enligt punkt 1 c är, som framgår ovan, en rättslig förpliktelse som är fastställd i enlighet med unionsrätten eller den nationella rätten. Vad gäller behandling som är nödvändig för att uppfylla en sådan rättslig förpliktelse ska alltså syftet med behandlingen vara bestämd av den författning som anger eller ger stöd för förpliktelsen. En rättslig förpliktelse utgör därmed inte en rättslig grund för behandling av personuppgifter om förpliktelsen är alltför svepande och ger den personuppgiftsansvarige en alltför stor handlingsfrihet i fråga om hur den ska uppfyllas. Som exempel kan nämnas att ett företags skyldighet att lämna uppgift om företagets lönekostnader inte innehåller något angivet syfte för behandling av personuppgifter i form av utlämnande, medan en skyldighet att lämna

⁹ SOU 1997:39 s. 363.

uppgifter om företagets löneutbetalning till en angiven arbetstagare innehåller ett sådant syfte. Den senare förpliktelsen kan i praktiken inte uppfyllas utan att personuppgifter rörande den angivna arbetstagaren behandlas.

Detta krav är i sig ingen nyhet, men framgår inte uttryckligen av dataskyddsdirektivet. Artikel 29-gruppen har i ett yttrande avseende begreppet rättslig förpliktelse i artikel 7 c i dataskyddsdirektivet anfört att den bestämmelse som förpliktelsen grundas på ska innehålla en uttrycklig hänvisning till arten av och syftet med behandlingen. Artikel 29-gruppen anför följande.¹⁰

Dessutom måste den rättsliga förpliktelsen i sig vara tillräckligt tydlig när det gäller den behandling av personuppgifter som krävs. Artikel 7 c kan således tillämpas på grundval av rättsliga bestämmelser som innehåller en uttrycklig hänvisning till arten av och syftet med behandlingen. De registeransvariga bör inte ges en alltför stor handlingsfrihet i fråga om hur de ska uppfylla den rättsliga förpliktelsen.

I vissa fall anger lagstiftningen kanske bara ett allmänt mål, medan mer specifika förpliktelser införs på en annan nivå, till exempel antingen genom sekundärlagstiftning eller genom ett bindande beslut av en offentlig myndighet i ett konkret fall. Detta kan också leda till rättsliga förpliktelser enligt artikel 7 c, förutsatt att arten och syftet med behandlingen är väl definierade och omfattas av en lämplig rättslig grund.

Hur fastställs rättsliga förpliktelser i enlighet med gällande rätt?

I Sverige följer det av grundlag att den offentliga makten utövas under lagarna (1 kap. 1 § tredje stycket regeringsformen). Offentlig-rättsliga förelägganden och beslut som medför förpliktelser för mottagaren ska därför ha sin grund i en författning. Förpliktelser som har en generell räckvidd, och alltså inte riktas mot en specifik mottagare, ska också regleras i författning. Detta gäller både offentlig-rättsliga och civilrättsliga åligganden. Som tidigare har nämnts bör däremot civilrättsliga förpliktelser som följer av avtal där den registrerade själv är part i stället bedömas i enlighet med den särskilda rättsliga grunden i artikel 6.1 b i dataskyddsförordningen.

Som en följd av den svenska arbetsmarknadsmodellen kan rättsliga förpliktelser även anges i kollektivavtal. Sådana avtal omfattas

¹⁰ Artikel 29-gruppens yttrande 6/2014 om begreppet den registeransvariges berättigade intressen enligt artikel 7 i direktiv 95/46/EG, s. 21.

inte av artikel 6.1 b, eftersom den registrerade inte själv är part. Förpliktelser som följer av kollektivavtal måste däremot enligt vår bedömning anses vara fastställda i enlighet med svensk rätt.

Enligt 8 kap. 2 § regeringsformen ska föreskrifter meddelas genom lag bland annat om de avser

1. enskildas personliga ställning och deras personliga och ekonomiska förhållanden inbördes,
2. förhållandet mellan enskilda och det allmänna under förutsättning att föreskrifterna gäller skyldigheter för enskilda eller i övrigt avser ingrepp i enskildas personliga eller ekonomiska förhållanden, eller
3. grunderna för kommunernas organisation och verksamhetsformer och för den kommunala beskattningen samt kommunernas befogenheter i övrigt och deras åligganden.

Enligt 8 kap. 3 § regeringsformen kan riksdagen, med vissa undantag, bemyndiga regeringen att meddela föreskrifter enligt 2 § första stycket 2 och 3. Om riksdagen bemyndigar regeringen att meddela föreskrifter i ett visst ämne, kan riksdagen också medge att regeringen bemyndigar en förvaltningsmyndighet eller en kommun att meddela föreskrifter i ämnet. Detta framgår av 8 kap. 10 § regeringsformen. Enligt 8 kap. 9 § regeringsformen kan riksdagen även bemyndiga en kommun att meddela föreskrifter enligt 2 § första stycket 2, om föreskrifterna avser t.ex. avgifter.

Det står således klart att rättsliga förpliktelser som åligger enskilda eller kommuner alltid ska ha sin grund i lag eller i kollektivavtal. Förpliktelser kan regleras direkt i lag eller i föreskrifter som meddelats med stöd av lag. Förpliktelser kan också anges i domar eller myndighetsbeslut som meddelats med stöd av lag eller med stöd av föreskrifter som i sin tur meddelats med stöd av lag.

På samma sätt har unionsrättsliga förpliktelser stöd i svensk lag, t.ex. förpliktelser som följer av direkt tillämpliga EU-förordningar eller som meddelas med stöd av sådana förordningar. Enligt lagen (1994:1500) med anledning av Sveriges anslutning till Europeiska unionen gäller nämligen EU-rättsakter här i landet med den verkan som följer av EU-fördragen.

Även domstolar och statliga myndigheter kan, vid sidan av sina uppgifter och uppdrag, sägas ha rättsliga förpliktelser. Det finns

ingenting i artikel 6.1 c i dataskyddsförordningen som begränsar tillämpningen till den privata sektorn. Datainspektionen har t.ex. ansett att den skyldighet för myndigheter som följer av offentlighetsprincipen är en sådan rättslig skyldighet som avses i motsvarande bestämmelse i personuppgiftslagen.¹¹ Domstolar och myndigheter har också andra författningsreglerade förpliktelser som i sig kräver personuppgiftsbehandling, exempelvis när det gäller personaladministration. Däremot har Datainspektionen ansett att innehållet i en myndighets arbetsordning normalt inte kan grunda en rättslig skyldighet att behandla personuppgifter.¹²

Enligt 1 kap. 6 § regeringsformen är det regeringen som styr riket. Under regeringen lyder Justitiekanslern och andra statliga förvaltningsmyndigheter som inte är myndigheter under riksdagen (12 kap. 1 § regeringsformen). Regeringen styr dessa myndigheter genom regeringsbeslut och genom att med stöd av restkompetensen (8 kap. 7 § första stycket 2 regeringsformen) meddela föreskrifter. En myndighets uppdrag enligt myndighetsinstruktionen eller regleringsbrevet kan i vissa fall utgöra en i enlighet med nationell rätt (regeringsformen) fastställd rättslig förpliktelse i dataskyddsförordningens mening, t.ex. om myndigheten ges i uppdrag att föra ett visst personuppgiftsregister. I normalfallet torde dock myndighetens uppdrag i första hand utgöra en rättslig grund för behandling av personuppgifter med stöd av artikel 6.1 e i dataskyddsförordningen, dvs. på grundval av att uppdraget avser en uppgift av allmänt intresse, se avsnitt 8.3.4.

Vår bedömning

Sammanfattningsvis bedömer vi att de rättsliga förpliktelser som kräver personuppgiftsbehandling, utan att någon annan rättslig grund är tillämplig, redan framgår av eller meddelas med stöd av gällande rätt. Det behövs därmed inte någon ytterligare nationell reglering på generell nivå för att sådan behandling av personuppgifter som är nödvändig för att uppfylla en rättslig förpliktelse ska kunna ske med stöd

¹¹ Datainspektionens rapport 2005:3, Övervakning i arbetslivet – Kontroll av de anställdas Internet- och e-postanvändning m.m., s. 15.

¹² Öman och Lindblom, Personuppgiftslagen, (20 december 2016, Zeteo), kommentaren till 10 § b PUL.

av den rättsliga grunden i artikel 6.1 c i dataskyddsförordningen. Detta gäller oavsett om den personuppgiftsansvarige är en myndighet eller ett privaträttsligt organ.

Det kan dock finnas anledning att ta in en bestämmelse i dataskyddslagen som tydliggör att en förpliktelse utgör en rättslig grund för behandling av personuppgifter endast om förpliktelsen gäller enligt lag eller annan författning eller följer av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Detta är enligt skäl 8 till dataskyddsförordningen förenligt med unionsrätten, även om åtgärden kan sägas utgöra ett införlivande av en direkt tillämplig förordningsbestämmelse.

För att en förpliktelse ska kunna läggas till grund för behandling av personuppgifter måste den givetvis vara rättsligt förankrad och giltig. Den måste alltså ha meddelats i laga ordning. Den föreslagna formuleringen ”gäller enligt lag” omfattar även förpliktelser som följer av direkt tillämpliga unionsrättsakter, eftersom lagen med anledning av Sveriges anslutning till Europeiska unionen anger att unionsrättsakter gäller här i landet med den verkan som följer av fördragen.

Det bör noteras att bestämmelsen i artikel 6.3 andra stycket första meningen i dataskyddsförordningen anger att syftet med behandlingen ska fastställas i den rättsliga grunden. Även denna bestämmelse är direkt tillämplig och kan möjligen begränsa tillämpningsområdet för artikel 6.1 c, jämfört med hur 10 § b PUL har tillämpats. Kravet torde enligt vår bedömning innebära att en förpliktelse inte kan läggas till grund för behandling av personuppgifter om syftet med behandlingen inte framgår av den författning som förpliktelsen grundas på och inte heller, i förekommande fall, kan utläsas av det beslut som anger förpliktelsen. Hur bestämmelsen ska tolkas och tillämpas i praktiken är dock i dagsläget oklart. Den närmare innebörden bör enligt vår uppfattning klargöras i rättspraxis.

8.3.3 Behandling som ett led i myndighetsutövning

Utredningens förslag: Det ska tydliggöras att personuppgifter får behandlas om behandlingen är nödvändig som ett led i myndighetsutövning som den personuppgiftsansvarige utövar enligt lag eller annan författning.

Begreppet myndighetsutövning

Enligt artikel 6.1 e i dataskyddsförordningen får personuppgifter behandlas bland annat om behandlingen är nödvändig som ett led i den personuppgiftsansvariges myndighetsutövning. Enligt dataskyddsdirektivet ska även behandling som är nödvändig som ett led i myndighetsutövning som utförs av en tredje man till vilken uppgifterna har lämnats ut tillåtas, men denna rättsliga grund nämns inte i dataskyddsförordningen. Av skäl 45 till dataskyddsförordningen framgår att det på unionsnivå eller nationellt bör regleras om en personuppgiftsansvarig som utför myndighetsutövning ska vara en myndighet eller någon annan som omfattas av offentligrättslig lagstiftning eller om denne kan vara en fysisk eller juridisk person som lyder under civilrättslig lagstiftning, t.ex. en yrkesorganisation.

Datalagskommittén bedömde att begreppet myndighetsutövning har en EG-gemensam innebörd, men att man till dess annat framkommer bör kunna utgå från att det som i Sverige brukar anses som myndighetsutövning faller under begreppet.¹³ Vi instämmer i denna bedömning. Termen används flitigt i svenska författningar, även i grundlag, men saknar legaldefinition. Begreppet som sådant har kritiserats, bland annat av Förvaltningslagsutredningen.¹⁴ I förarbetena till den äldre förvaltningslagen (1971:290) finns dock en beskrivning av begreppets innebörd som fortfarande ofta citeras.¹⁵

Myndighetsutövning mot enskilda karaktäriseras av beslut eller andra ensidiga åtgärder som ytterst är uttryck för samhällets maktbefogenheter i förhållande till medborgarna. Befogenheten till myndighetsutövning måste alltså vara grundad på lag eller annan författning eller på annat sätt kunna härledas ur bemyndiganden från de

¹³ SOU 1997:39 s. 365.

¹⁴ SOU 2010:29 s. 99 f.

¹⁵ Prop. 1971:30 s. 331 f.

högsta statsorganen. Myndighetsutövning kan både medföra förpliktelser för enskilda och mynna ut i gynnande beslut. Myndighetsutövning kan också ske i förhållandet mellan myndigheter, t.ex. när en myndighet har tillsyn över en annan myndighets verksamhet. Utanför begreppet myndighetsutövning faller däremot råd, upplysningar och andra inte bindande uttalanden samt sådan faktisk verksamhet som inte innebär tvång mot den enskilde (t.ex. undervisning). Gränsdragningen mellan offentligrättsliga och privaträttsliga regler är också av stor vikt när det gäller att bestämma begreppet myndighetsutövning.¹⁶

Av naturliga skäl är det i första hand statliga och kommunala myndigheter som ägnar sig åt myndighetsutövning. Även juridiska och fysiska personer kan dock med stöd av lag anförtros förvaltningsuppgifter som innefattar myndighetsutövning (12 kap. 4 § regeringsformen). Denna möjlighet har bland annat utnyttjats vad gäller betygssättning m.m. i fristående skolverksamhet och fordonsbesiktning som utförs av privaträttsliga besiktningsorgan.

Ändamålet med behandlingen måste vara nödvändigt

Enligt artikel 6.3 andra stycket första meningen i dataskyddsförordningen ska syftet med behandlingen (*the purpose of the processing*), i fråga om behandling enligt punkt 1 e, vara nödvändigt som ett led i den personuppgiftsansvariges myndighetsutövning. Ändamålet behöver således inte framgå av det sammanhang där den myndighetsutövande befogenheten fastställs. Ändamålet med behandlingen av personuppgifter måste dock vara nödvändigt för att utföra myndighetsutövningen. Bestämmelsen uttrycker det samband som måste finnas mellan behandlingen och myndighetsutövningen. Detta samband framgår även av kravet i artikel 5.1 b på att de särskilda ändamålen ska vara berättigade.

¹⁶ Lundell/Strömberg, Allmän förvaltningsrätt, 26 uppl., s. 19 f.

Är all myndighetsutövning fastställd i enlighet med gällande rätt?

I svensk rätt har myndigheter inte någon generell befogenhet att utöva myndighet. Myndighetsutövning som medför skyldigheter för den enskilde eller i övrigt avser ingrepp i den enskildes personliga eller ekonomiska förhållanden måste härröra från lag (8 kap. 2 § 2 och 3 § regeringsformen). Att meddela föreskrifter om åtgärder som är gynnande för den enskilde ryms däremot inom regeringens restkompetens (8 kap. 7 § första stycket 2 regeringsformen). Regeringen kan därmed i förordning, utan bemyndigande av riksdagen, ge en myndighet befogenheter avseende gynnande myndighetsutövning. Myndighetsutövning kan däremot inte ske helt utan stöd av författning. Det bör vidare noteras att myndighetsutövning även kan utövas med stöd av direkt tillämpliga EU-förordningar. Myndighetsutövning kan således även vara fastställd i enlighet med unionsrätten.

Befogenhet att utföra myndighetsutövande förvaltningsuppgifter fastställs i svensk rätt ofta direkt i den författning som reglerar en viss rättighet, skyldighet, åtgärd eller verksamhet.¹⁷ Befogenheten kan även framgå genom att en myndighet i lag eller förordning har pekats ut att fullgöra de uppgifter som ankommer på behörig myndighet enligt en viss unionsrättsakt.¹⁸ I det sistnämnda fallet kan de myndighetsutövande uppgifterna vara uttryckta enbart i unionsrätten. Myndighetsutövning kan dock aldrig utövas utan stöd i gällande rätt.

Enligt skäl 45 till dataskyddsförordningen bör unionsrätten eller den nationella rätten också reglera frågan om en personuppgiftsansvarig som utför myndighetsutövning ska vara ett organ som omfattas av offentligrättslig eller av civilrättslig lagstiftning. I Sverige regleras myndighetsutövande uppgifter i offentligrättslig lagstiftning. Det innebär inte att det bara är myndigheter som har anförtrotts sådana uppgifter. Däremot krävs lagstöd för att förvaltningsuppgifter som innefattar myndighetsutövning ska kunna överlämnas åt andra juridiska personer och enskilda individer (12 kap. 4 § regeringsformen). Frågan om vilka organ som har myndighetsutövande uppgifter regleras således redan i svensk rätt.

¹⁷ Se t.ex. studiestödslagen (1999:1395), skatteförfarandelagen (2011:1244), plan- och bygglagen (2010:900) eller lagen (2009:366) om handel med läkemedel.

¹⁸ Se t.ex. förordningen (2009:93) med instruktion för Finansinspektionen eller förordningen (2007:860) med instruktion för Statens haverikommission.

Vår bedömning

I Sverige kan myndighetsutövning inte ske utan stöd i gällande rätt. Det krävs därför inte någon ny nationell reglering på generell nivå för att sådan behandling av personuppgifter som är nödvändig som ett led i den personuppgiftsansvariges myndighetsutövning ska kunna ske med stöd av den rättsliga grunden i artikel 6.1 e i förordningen. Det bör noteras att denna rättsliga grund för behandling av personuppgifter kan tillämpas av alla personuppgiftsansvariga som tilldelats myndighetsutövande befogenheter.

Det kan dock finnas anledning att ta in en bestämmelse i dataskyddslagen som tydliggör att myndighetsutövning utgör en rättslig grund för behandling av personuppgifter endast om myndighetsutövningen sker enligt lag eller annan författning. Detta är enligt skäl 8 till dataskyddsförordningen förenligt med unionsrätten, även om åtgärden kan sägas utgöra ett införlivande av en direkt tillämplig förordningsbestämmelse.

8.3.4 Behandling för att utföra uppgifter av allmänt intresse

Utredningens förslag: Det ska tydliggöras att personuppgifter får behandlas om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna utföra en uppgift av allmänt intresse som följer av lag eller annan författning eller av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning.

Begreppet uppgift av allmänt intresse

Enligt artikel 6.1 e i dataskyddsförordningen får personuppgifter behandlas om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse. Av skäl 45 till dataskyddsförordningen framgår att det på unionsnivå eller nationellt bör regleras om en personuppgiftsansvarig som utför en uppgift av allmänt intresse ska vara en myndighet eller någon annan som omfattas av offentligrättslig lagstiftning eller om denne kan vara en fysisk eller juridisk person som lyder under civilrättslig lagstiftning, t.ex. en yrkesorganisation.

Begreppet allmänt intresse är ett unionsrättsligt begrepp som inte med enkelhet låter sig avgränsas. Begreppet definieras varken i data-

skyddsdirektivet eller i dataskyddsförordningen och dess innebörd har ännu inte heller utvecklats av EU-domstolen. Artikel 29-gruppen har dock inrättat en arbetsgrupp som har fått i uppgift att utarbeta och revidera vägledande yttranden rörande vissa nyckelbestämmelser och begrepp i förordningen.¹⁹ Förhoppningsvis kommer begreppet uppgift av allmänt intresse att belysas i detta arbete.

Som exempel på uppgifter som kan vara av allmänt intresse nämns i Datalagskommitténs betänkande arkivering, forskning och framställning av statistik, etablerade idrottsorganisationers registrering av vilka personer som har vunnit svenska mästerskap eller innehar svenskt rekord i erkända sportgrenar, samt registrering av personer som har fått allmänt erkända utmärkelser såsom Nobelpris. Att någon själv kan tjäna pengar på att utföra uppgiften utesluter enligt Datalagskommittén inte att den ändå kan vara av allmänt intresse, såsom när uppgifter som tidigare skötts av det allmänna läggs ut på privata företag som drivs i vinstsyfte.²⁰

Möjligen har den behandling av personuppgifter som är nödvändig i t.ex. myndigheternas verksamhet i vissa fall ansetts vara tillåten endast efter en intresseavvägning enligt 10 § f PUL. Den motsvarande bestämmelsen i dataskyddsförordningen, artikel 6.1 f, ska dock inte gälla för behandling som utförs av offentliga myndigheter när de utför sina uppgifter. Myndigheternas utrymme för att grunda behandling på samtycke från den registrerade kan också antas minska. I skäl 43 anges nämligen att samtycke inte bör utgöra giltig grund för behandling i de fall där det råder betydande ojämlikhet mellan den registrerade och den personuppgiftsansvarige, särskilt om den personuppgiftsansvarige är en offentlig myndighet och det därför är osannolikt att samtycket har lämnats frivilligt när det gäller alla förhållanden som denna särskilda situation omfattar. För att myndigheternas verksamhet ska kunna fungera även i fortsättningen anser vi mot denna bakgrund att mycket talar för att begreppet uppgift av allmänt intresse måste anses ha fått en vidare unionsrättslig betydelse genom dataskyddsförordningen än det hittills har haft.

¹⁹ Artikel 29-gruppens Work programme 2016–2018, dok. 417/16/EN.

²⁰ SOU 1997:39 s. 364.

Myndigheternas uppdrag och åligganden att utföra uppgifter av allmänt intresse

Rent språkligt kan begreppet uppgift av allmänt intresse antas avse något som är av intresse för eller berör många människor på ett bredare plan, i motsats till ett särintresse. Av skäl 45 till förordningen följer att allmänintresset inbegriper hälso- och sjukvårdsändamål, folkhälsa, socialt skydd och förvaltning av hälso- och sjukvårdstjänster.

I avsaknad av vägledande domar från EU-domstolen förefaller det med hänsyn till svensk förvaltningstradition rimligt att anta att alla uppgifter som utförs av statliga myndigheter i syfte att uppfylla ett uttryckligt uppdrag av riksdag eller regering är av allmänt intresse. På motsvarande sätt bör man kunna utgå från att de obligatoriska uppgifter som utförs av kommuner och landsting, till följd av deras åligganden enligt lag eller förordning, är av allmänt intresse i dataskyddsförordningens mening.

Sådana uppgifter, som alltså utförs i syfte att utföra ett uttryckligt uppdrag eller till följd av ett åliggande, bör anses vara av allmänt intresse oavsett om de faktiskt utförs i myndighetens egen regi, av egna anställda, eller om de genom utkontraktering utförs av någon annan. När en juridisk eller fysisk person, på uppdrag av en kommunal eller statlig myndighet, utför en förvaltningsuppgift som åligger kommunen eller myndigheten, bör alltså entreprenören anses utföra en uppgift av allmänt intresse. Den omständigheten att entreprenören bedriver en rent kommersiell verksamhet kan under sådana omständigheter inte påverka bedömningen av den aktuella uppgiftens art.²¹

Andra uppgifter som utförs av myndigheter

Begreppet uppgifter av allmänt intresse omfattar dock inte bara sådant som utförs som en följd av ett offentligrättsligt och uttryckligt åliggande eller uppdrag. Till skillnad från vad som gäller enligt artikel 6.1 c i dataskyddsförordningen behöver den personuppgiftsansvarige inte vara skyldig att utföra uppgiften för att den rättsliga grunden i led e ska vara tillämplig. Däremot måste behandlingen vara nödvändig.

²¹ För ett liknande resonemang, se artikel 29-gruppens yttrande 6/2014 om begreppet den registeransvariges berättigade intressen enligt artikel 7 i direktiv 95/46/EG, s. 23, not 42.

Som en följd av det kommunala självstyret har kommuner och landsting en vidsträckt möjlighet att göra frivilliga åtaganden. Befogenheten är emellertid begränsad till angelägenheter av allmänt intresse (2 kap. 1 § kommunallagen [1991:900]). Kommuner och landsting får driva näringsverksamhet, men bara om den drivs utan vinstsyfte och går ut på att tillhandahålla allmännyttiga anläggningar eller tjänster åt medlemmarna i kommunen eller landstinget (2 kap. 7 § kommunallagen). Som exempel på sådana uppgifter av allmänt intresse som kommunerna utför på frivillig grund kan nämnas tillhandahållande av bostäder och fritids- och idrottsanläggningar, åtgärder för att främja ortens näringsliv och annan kulturell verksamhet än bibliotek (som i stället är en obligatorisk uppgift). Fullmäktige ska enligt 6 kap. 32 § första stycket kommunallagen utfärda reglementen med närmare föreskrifter om nämndernas verksamhet och arbetsformer. Även sådana frivilliga åtaganden som en kommun gör inom ramen för sin allmänna befogenhet ska således framgå av den ansvariga nämndens reglemente.

Vissa myndigheter, t.ex. Lantmäteriet, har uttryckligen getts befogenhet att bedriva viss uppdragsverksamhet.²² Även denna typ av verksamhet kan vara motiverad av ett allmänt intresse.

Uppgifter av allmänt intresse som utförs av privaträttsliga organ

De senaste årens avmonopolisering och konkurrensutsättning av offentlig verksamhet har inneburit att privaträttsliga organ numera utför en inte obetydlig del av de uppgifter som måste anses vara av allmänt intresse, även i begreppets mest snäva bemärkelse. Detta gäller inom den kommunala sektorn exempelvis avseende barnomsorg och skola, hälso- och sjukvård och stöd och service till funktionshindrade. Inom den traditionellt statliga sektorn kan nämnas järnvägstransporter, elektronisk kommunikation, postbefordran och elproduktion. Ibland bedrivs verksamheten alltjämt under kommunal eller statlig styrning, i form av kommunala eller statliga bolag, men på andra områden förekommer också eller enbart privata subjekt som är associationsrättsligt helt fristående från den offentliga sektorn.

²² 10 och 12 §§ förordningen (2009:946) med instruktion för Lantmäteriet. Se även t.ex. 2 a § förordningen (2009:1394) med instruktion för Statens veterinärmedicinska anstalt eller 3 § förordningen (2007:1111) med instruktion för Patent- och registreringsverket.

Fysiska personer, ideella och ekonomiska föreningar, stiftelser och företag kan förstås också ägna sig åt annan verksamhet som i princip skulle kunna anses vara av allmänt intresse, t.ex. idrott och kultur, värme- och livsmedelsproduktion och tillhandahållande av finansiella tjänster, kreditupplysning eller transporter.

Genom regleringskravet avgränsas tillämpningsområdet

Vilka uppgifter som ska anses vara av allmänt intresse i dataskyddsförordningens mening är inte helt uppenbart. Den osäkerhet som råder avseende begreppets innebörd är dock ingen nyhet.

Däremot innebär dataskyddsförordningen en väsentlig förändring på så sätt att det inte längre är självklart att en personuppgiftsansvarig som utför en uppgift av allmänt intresse kan utföra nödvändig behandling av personuppgifter på den grunden. Genom kravet på att grunden för behandlingen ska fastställas i enlighet med unionsrätten eller den nationella rätten begränsas nämligen tillämpningsområdet för artikel 6.1 e. Det räcker inte att en behandling av personuppgifter är nödvändig för att utföra en uppgift av allmänt intresse – uppgiften måste också vara fastställd i enlighet med gällande rätt.

Regleringskravet i artikel 6.3 första stycket i dataskyddsförordningen innebär alltså att artikel 6.1 e inte kan åberopas i alla situationer då behandling av personuppgifter är nödvändig för att utföra en uppgift av allmänt intresse. Kravet på att grunden för behandlingen ska fastställas medför att uppgiften måste vara reglerad i enlighet med unionsrätten eller den nationella rätten. I skäl 45 till dataskyddsförordningen anges att förordningen inte medför något krav på en särskild lag för varje enskild behandling, utan att det kan räcka med en lag som grund för flera behandlingar som krävs för att utföra en uppgift av allmänt intresse.

Ändamålet med behandlingen måste vara nödvändigt

Enligt artikel 6.3 andra stycket första meningen i dataskyddsförordningen ska syftet med behandlingen (*the purpose of the processing*), i fråga om behandling enligt punkt 1 e, vara nödvändigt för att utföra en uppgift av allmänt intresse. Till skillnad mot vad som gäller avseende grunden rättslig förpliktelse behöver ändamålet således inte

framgå av den författning eller det beslut där själva uppgiften fastställs. Ändamålet med varje enskild behandling måste dock vara nödvändigt för att utföra den fastställda uppgiften. Bestämmelsen uttrycker det samband som måste finnas mellan behandlingen och den fastställda uppgiften och riktar sig till den som bestämmer de särskilda ändamålen för behandlingen, vilket i normalfallet är den personuppgiftsansvarige men i vissa fall även kan vara lagstiftaren. Detta krav på samband framgår även av artikel 5.1 b, där det anges att de särskilda ändamålen ska vara berättigade.

Som exempel kan nämnas att det enligt 3 § bibliotekslagen (2013:801) fastställs att kommunerna ansvarar för folkbibliotek. I 9 § bibliotekslagen anges att allmänheten avgiftsfritt ska få låna eller på annat sätt få tillgång till litteratur under en viss tid oavsett publiceringsform. Man skulle förstås kunna tänka sig att biblioteken skulle låna ut böcker, utan att veta vilka låntagarna är. Det förefaller dock föga lämpligt, eftersom det kan antas att böcker då inte skulle lämnas tillbaka. Det bör därför kunna anses nödvändigt, i unionsrättslig mening, för biblioteken att samla in personuppgifter från dem som lånar böcker, i syfte att föra ett register över låntagare och deras lån. Detta ändamål är därmed nödvändigt för att utföra uppgiften, att bedriva biblioteksverksamhet. Behandlingen av personuppgifter kan således ske enligt artikel 6.1 e, på den rättsliga grund som utgörs av bibliotekslagen.²³

Alla myndigheter, såväl statliga som kommunala, utför en rad administrativa uppgifter som krävs för att myndigheten ska fungera, men som varken direkt eller indirekt kan sägas framgå av uppdraget. Som exempel kan nämnas myndigheternas säkerhetsarbete. I skäl 27 till den rättsakt som gäller för EU-institutionernas personuppgiftsbehandling, förordning 45/2001, anges att behandling av personuppgifter för utförandet av de uppgifter av allmänt intresse som gemenskapsinstitutionerna och gemenskapsorganen utför inbegriper sådan behandling av personuppgifter som är nödvändig för förvaltningen av dessa institutioner och organ för att de ska fungera. Enligt artikel 29-

²³ I praktiken måste den personuppgiftsansvarige givetvis även säkerställa att behandlingen uppfyller principerna i artikel 5, bland annat att ändamålet är berättigat enligt led b och att personuppgifterna behandlas *fairly* enligt led a.

gruppen möjliggör skäl 27 en vid tolkning av begreppet allmänt intresse i förordning 45/2001.²⁴

Någon motsvarighet till skäl 27 i förordning 45/2001 finns inte i den nya dataskyddsförordningen. Under förhandlingarna av förordningen har dock Artikel 29-gruppen gett uttryck för att grunderna allmänt intresse och myndighetsutövning måste tolkas på samma sätt som i förordning 45/2001, nämligen på ett sådant sätt att de offentliga myndigheterna ges en viss grad av flexibilitet, åtminstone så att myndigheternas förvaltning och funktion säkerställs.²⁵

Vår bedömning

Myndigheter

Statliga och kommunala myndigheters verksamhet är i allt väsentligt av allmänt intresse. Det är därmed den rättsliga grunden i artikel 6.1 e i dataskyddsförordningen som vanligen bör tillämpas av myndigheter, även utanför området för myndighetsutövning. Viss behandling av personuppgifter är dock även nödvändig med anledning av avtal, t.ex. när det gäller rekryteringsärenden eller inköp, och kan därmed också ske med stöd av den rättsliga grunden avseende just avtal (artikel 6.1 b). Denna rättsliga grund kan i vissa fall även tillämpas av de myndigheter som uttryckligen har getts befogenhet att bedriva uppdragsverksamhet. En myndighet kan också behöva behandla personuppgifter för att uppfylla en rättslig förpliktelse, t.ex. att föra ett visst register eller gentemot Skatteverket i egenskap av arbetsgivare eller till följd av offentlighetsprincipen (artikel 6.1 c). Undantagsvis kan det även förekomma behov av behandling av personuppgifter för att skydda intressen av grundläggande betydelse för fysisk person (artikel 6.1 d). Myndigheter kan däremot inte åberopa den rättsliga grund som utgår från en intresseavvägning (artikel 6.1 f) när de fullgör sina uppgifter.

Myndigheternas uppdrag och åligganden framgår av författningar, regeringsbeslut och kommunala reglementen, antagna i enlighet med grundlagens bestämmelser om normgivningskompetens och kommu-

²⁴ Artikel 29-gruppens yttrande 6/2014 om begreppet den registeransvariges berättigade intressen enligt artikel 7 i direktiv 95/46/EG, s. 24.

²⁵ Se föregående fotnot.

nalt självstyre. De åtgärder som myndigheterna vidtar i syfte att utföra dessa uppdrag eller uppfylla dessa åligganden har därmed i sig en legal grund, som har offentliggjorts genom tydliga, precisa och förutsebara regler. Nödvändig behandling av personuppgifter kan därmed ske med stöd av artikel 6.1 e i dataskyddsförordningen. Någon ytterligare reglering av myndigheternas obligatoriska uppgifter krävs därmed inte på generell nivå för att myndigheter ska kunna vidta nödvändiga behandlingsåtgärder för att fullgöra sina uppgifter.

I artikel 6.3 andra stycket anges att syftet med behandlingen måste vara nödvändigt för att utföra uppgiften. Den specifika behandlingen måste alltså vara nödvändig för ett ändamål som i sin tur är nödvändigt för att myndigheten ska kunna utföra sitt uppdrag. Om myndigheten inte fungerar kan den inte utföra sina fastställda uppgifter. Även administrativa åtgärder som är nödvändiga för myndighetens förvaltning och funktion är därmed rättsligt grundade i dataskyddsförordningens mening.

Det kan inte nog betonas att rättslig grund inte är en tillräcklig förutsättning för att behandling av personuppgifter ska vara tillåten. Behandlingen är laglig endast i den mån den faktiskt är nödvändig för att utföra uppgiften. Dessutom måste behandlingen följa de övriga krav som ställs i dataskyddsförordningen, till exempel de principer för behandlingen som anges i artikel 5. I sammanhanget vill vi särskilt peka på att behandlingen enligt artikel 5.1 a ska vara korrekt, i betydelsen skälig eller rimlig (*fairly*), i förhållande till den registrerade. Behovet av den konkreta behandlingen måste alltså alltid vägas emot den registrerades rätt till skydd för sina personuppgifter.

Privata aktörer

Uppdrag från en myndighet

Som tidigare har nämnts anser vi att de uppgifter av allmänt intresse som utförs i syfte att utföra ett uttryckligt uppdrag eller till följd av ett åliggande, måste anses vara av allmänt intresse oavsett om de faktiskt utförs i myndighetens egen regi, av egna anställda, eller om de genom utkontraktering utförs av någon annan. När en juridisk eller fysisk person, på uppdrag av en kommunal eller statlig myndighet, utför en förvaltningsuppgift som åligger kommunen eller myndigheten, bör alltså även den privata utföraren, entreprenören eller det

kommunala bolaget anses utföra en uppgift av allmänt intresse. Ett privaträttsligt organ som fullgör ett uppdrag från en myndighet avseende en sådan uppgift som är fastställd i författning, regeringsbeslut eller kommunalt beslut i fullmäktige kan därför vidta nödvändiga behandlingsåtgärder på samma rättsliga grund som om myndigheten själv utfört uppgiften, dvs. med stöd av artikel 6.1 e i dataskyddsförordningen.

Det bör noteras att en uppdragstagare som utgör personuppgiftsbiträde åt myndigheten i stället behandlar personuppgifter med stöd av artikel 28 i dataskyddsförordningen, i enlighet med den personuppgiftsansvariges instruktioner.

Verksamhet som omfattas av handlingsoffentlighet

I artikel 86 i dataskyddsförordningen anges att personuppgifter i allmänna handlingar som förvaras av en myndighet eller ett offentligt organ eller ett privat organ för utförande av en uppgift av allmänt intresse får lämnas ut av myndigheten eller organet i enlighet med den unionsrätt eller den medlemsstats nationella rätt som myndigheten eller organet omfattas av, för att jämka samman allmänhetens rätt att få tillgång till allmänna handlingar med rätten till skydd av personuppgifter i enlighet med denna förordning. Bestämmelsen bör enligt vår mening tolkas så att den svenska offentlighetsprincipen har företräde framför dataskyddsförordningen avseende dels handlingar som förvaras hos myndigheter och andra offentliga organ, dels sådana handlingar som förvaras hos privata organ för utförande av en uppgift av allmänt intresse. Offentlighetsprincipen skulle däremot inte kunna ges företräde framför dataskyddsförordningen när det gäller handlingar som förvaras hos privata organ av något annat skäl än för utförande av en uppgift av allmänt intresse.

Enligt 2 kap. 2–5 §§ offentlighets- och sekretesslagen (2009:400, förkortad OSL,) ska vad som föreskrivs i tryckfrihetsförordningen om rätt att ta del av allmänna handlingar hos myndigheter i tillämpliga delar också gälla hos bland annat kommunala bolag och de organ som anges i bilagan till offentlighets- och sekretesslagen, om handlingarna hör till den verksamhet som nämns där. Enligt vår mening måste dessa organ, vars handlingar omfattas av handlingsoffentlighet, i motsvarande utsträckning anses utföra uppgifter av allmänt intresse

i den mening som avses i dataskyddsförordningen. De uppgifter som dessa organ utför är fastställda i dataskyddsförordningens mening, i den mån uppgifterna anges i författningar, regeringsbeslut och kommunala beslut av fullmäktige (t.ex. ägardirektiv). Nödvändig behandling av personuppgifter som utförs av dessa organ för att utföra dessa uppgifter har därför en rättslig grund och är laglig enligt artikel 6.1 e i dataskyddsförordningen.

Övrig privaträttsligt bedriven verksamhet av allmänt intresse

Vid en direkt tillämpning av artikel 6.1 c och e spelar det ingen roll om den personuppgiftsansvarige är en offentlig eller en privat aktör. Om den uppgift som den personuppgiftsansvarige utför är av allmänt intresse och denna uppgift är fastställd i enlighet med unionsrätten eller den nationella rätten finns en rättslig grund för nödvändig behandling enligt artikel 6.1 e. Det spelar då heller ingen roll om verksamheten utförs på direkt uppdrag av en myndighet eller på eget initiativ.

Som tidigare har nämnts är uttrycket uppgift av allmänt intresse ett unionsrättsligt begrepp som hittills saknar definition. Det är därför mycket vanskligt att bedöma i vilken mån privaträttsligt bedriven verksamhet är av allmänt intresse i dataskyddsförordningens mening. De senaste årens avmonopolisering och konkurrensutsättning av offentlig verksamhet i Sverige har dock inneburit att privaträttsliga organ numera utför en inte obetydlig del av de uppgifter som sannolikt skulle anses vara av allmänt intresse, även i begreppets mest snäva bemärkelse. Detta gäller inom den kommunala sektorn exempelvis avseende barnomsorg och skola, hälso- och sjukvård samt stöd och service till funktionshindrade. Inom den traditionellt statliga sektorn kan nämnas järnvägstransporter, elektronisk kommunikation, postbefordran och eldistribution.

I flera av dessa nämnda fall är verksamheten av kommersiell karaktär och bygger på avtal med den registrerade (t.ex. järnvägstransporter eller eldistribution). I den mån behandling av personuppgifter är nödvändig kan den därmed ske med stöd av artikel 6.1 b i dataskyddsförordningen, även om uppgiften inte skulle vara fastställd i lagstiftningen. När det gäller hälso- och sjukvårdsverksamhet, i både offentlig och privat regi, fastställs uppgiften i bland annat hälso- och

sjukvårdslagen (2017:30), medan patientdatalagen (2008:355) specificerar villkoren för laglig behandling av personuppgifter. På motsvarande sätt regleras uppgiften att tillhandahålla stöd och service till funktionshindrade av lagen (1993:387) om stöd och service till vissa funktionshindrade, som också innehåller ett par dataskyddsbestämmelser som gäller även för privata utförare. I övrigt återfinns sektors-specifika bestämmelser om behandling av personuppgifter i lagen (2001:454) om behandling av personuppgifter inom socialtjänsten. Skolväsendets uppgifter fastställs i skollagen (2010:800), som gäller för både offentliga och enskilda anordnare av utbildning. Någon särskild registerförfattning som specificerar villkoren för behandling av personuppgifter på skolområdet finns dock inte, vilket innebär att det endast är dataskyddsförordningen som ska tillämpas.

När det är tveksamt om den verksamhet som en privaträttslig aktör bedriver är av allmänt intresse i unionsrättslig mening är det i stället ofta möjligt att grunda nödvändig behandling av personuppgifter på en intresseavvägning i enlighet med artikel 6.1 f i dataskyddsförordningen eller att inhämta den registrerades samtycke. Detsamma gäller om verksamheten visserligen är av allmänt intresse, men uppgiften inte är fastställd i enlighet med vare sig unionsrätten eller den nationella rätten. Det är dock inte uteslutet att det finns sådana oreglerade områden som bör bli föremål för reglering just med anledning av dataskyddsförordningen.

Behov av förtydligande

För att behandling av personuppgifter ska vara laglig enligt artikel 6.1 e i dataskyddsförordningen måste den uppgift som den personuppgiftsansvarige utför dels vara av allmänt intresse (eller utgöra ett led i myndighetsutövning), dels vara fastställd i enlighet med unionsrätten eller den nationella rätten. Vidare måste behandlingen vara nödvändig för ett ändamål som är nödvändigt för att utföra uppgiften. Detta framgår av direkt tillämpliga bestämmelser i dataskyddsförordningen. Det behövs därmed inte någon ytterligare nationell reglering, på generell nivå, för att sådan behandling av personuppgifter som är nödvändig för att utföra uppgifter av allmänt intresse ska kunna ske med stöd av den rättsliga grunden i artikel 6.1 e i för-

ordningen. Detta gäller oavsett om den personuppgiftsansvarige är en offentlig eller en privat aktör.

Det kan dock finnas anledning att ta in en bestämmelse i dataskyddslagen som tydliggör att begreppet uppgift av allmänt intresse avser en uppgift av allmänt intresse som utförs med stöd av gällande rätt. Uppgiften måste alltså följa av lag eller annan författning eller av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. En sådan upplysningsbestämmelse bidrar till förståelsen av dataskyddsregleringen och kan mot bakgrund av skäl 8 i förordningen inte anses vara en otillåten implementeringsåtgärd.

Det bör noteras att den författning eller det beslut som utgör den rättsliga grunden för behandling av personuppgifter måste uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas (artikel 6.3 andra stycket sista meningen i dataskyddsförordningen). Det finns därmed en bortre gräns för vilka uppgifter som över huvud taget kan läggas till grund för behandling av personuppgifter. Som exempel skulle det inte betraktas som proportionellt att ge en myndighet i uppgift att övervaka befolkningens kommunikation på internet, i syfte att upptäcka trakasserier. Ett åliggande för kommunerna att t.ex. inrätta särskilda skolor för barn vars föräldrar tillhör en viss religiös grupp, i syfte att förbättra skolresultaten, skulle på motsvarande sätt inte kunna utgöra rättslig grund för behandling av personuppgifter, eftersom uppgiften inte skulle anses proportionell.

8.3.5 Särskilda bestämmelser som anpassar tillämpningen av dataskyddsförordningen

Utrymmet för nationell specificering

Artikel 6.3 andra stycket i dataskyddsförordningen ger, i likhet med artikel 6.2, ett visst utrymme för medlemsstaterna att specificera villkoren för när behandling av personuppgifter får ske och hur det ska gå till. I artikel 6.3 andra stycket i dataskyddsförordningen anges nämligen att den rättsliga grund som fastställer en rättslig förpliktelse, myndighetsutövning eller en uppgift av allmänt intresse kan innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen. Som exempel nämns de allmänna villkor som ska gälla för den personuppgiftsansvariges behandling, vilken typ

av uppgifter som ska behandlas, vilka registrerade som berörs, de enheter till vilka personuppgifterna får lämnas ut och för vilka ändamål, ändamålsbegränsningar, lagringstid samt typer av behandling och förfaranden för behandling, inbegripet åtgärder för att tillförsäkra en laglig och rättvis behandling, däribland för behandling i andra särskilda situationer enligt kapitel IX. Av skäl 10 framgår att förordningen inte utesluter att det i medlemsstaternas nationella rätt fastställs närmare omständigheter för specifika situationer där uppgifter behandlas, inbegripet mer exakta villkor för laglig behandling av personuppgifter.

Bestämmelsen i artikel 6.3 andra stycket innebär ingen skyldighet för medlemsstaterna att införa sådana särskilda nationella bestämmelser. I svensk rätt finns det dock redan åtskilliga sådana särskilda dataskyddsbestämmelser i sektorspecifika registerförfattningar. Det är mycket vanligt att frågor om behandling av personuppgifter regleras i den offentlighetsrättsliga författning som i första hand annars har till syfte att reglera vem som får utföra en viss uppgift eller hur en viss verksamhet ska bedrivas, t.ex. socialförsäkringsbalken, alkohollagen (2010:1622) eller konkurslagen (1987:682).²⁶ Ibland återfinns dock alla dataskyddsbestämmelser avseende en viss verksamhet i särskilda informationshanteringsförfattningar, t.ex. patientdatalagen eller utlänningsdatalagen (2016:27). Det förekommer också renodlade registerförfattningar, t.ex. lagen (2001:558) om vägtrafikregister eller lagen (1996:1156) om receptregister. Samtliga dessa författningstekniker bör enligt vår bedömning kunna användas även fortsättningsvis för att vid behov specificera villkoren för behandling av personuppgifter, enligt både artikel 6.2 och artikel 6.3 andra stycket i dataskyddsförordningen.

Det bör noteras att bestämmelser som specificerar villkoren för laglig behandling, om medlemsstaten väljer att behålla eller införa sådana, måste uppfylla ett mål av allmänt intresse och vara proportionella mot det legitima mål som eftersträvas (artikel 6.3 andra stycket sista meningen i dataskyddsförordningen). Lagstiftaren måste alltså göra en avvägning mellan å ena sidan behovet av att uppgiften kan utföras på ett effektivt och rättssäkert sätt och, å andra sidan, den enskildes rätt till skydd för sina personuppgifter.

²⁶ Enligt Informationshanteringsutredningen finns det mer än ett hundratal författningar som hör till denna kategori, SOU 2015:39 s. 103 f.

Sådana särskilda bestämmelser som avses i artikel 6.3 andra stycket kräver att lagstiftaren gör avvägningar från fall till fall och kan enligt vår bedömning inte föras in på generell nivå. Vi lämnar därför inget sådant förslag.

8.3.6 Inledande upplysningsbestämmelse

Utredningens förslag: Dataskyddslagen ska innehålla en bestämmelse som erinrar om att dataskyddsförordningen anger att personuppgifter får behandlas endast om minst ett av de villkor som anges i artikel 6.1 i förordningen är uppfyllt.

För förståelsen av de ovan föreslagna bestämmelserna om tillämpningen av artikel 6.1 c och e i dataskyddsförordningen behövs det enligt vår bedömning en inledande upplysningsbestämmelse som erinrar läsaren om att personuppgifter får behandlas bara om det finns en rättslig grund, dvs. om minst ett av de villkor som anges i artikel 6.1 i dataskyddsförordningen är uppfyllt.

8.4 Sammanfattning

Behandling av personuppgifter måste ske på rättslig grund. De rättsliga grunder som godtas enligt artikel 6.1 i dataskyddsförordningen är

- samtycke (a)
- avtal (b)
- rättslig förpliktelse (c)
- vitala intressen (d)
- myndighetsutövning (e)
- uppgift av allmänt intresse (e), och
- berättigat intresse (f).

För tillämpning av leden b–f krävs att behandlingen är *nödvändig* för att fullgöra, skydda eller utföra den rättsliga grunden eller, i fråga om led f, för ändamål som rör den rättsliga grunden.

För *led a* finns särskilda villkor som måste vara uppfyllda, bland annat när det gäller barns samtycke (artikel 7 och 8).

För *leden c och e* krävs att den rättsliga grunden, dvs. den rättsliga förpliktelsen, myndighetsutövningen eller uppgiften av allmänt intresse, är *fastställd* i enlighet med nationell rätt eller unionsrätt (artikel 6.3 första stycket). En rättslig förpliktelse är enligt svensk rätt fastställd om den gäller enligt lag eller annan författning eller följer av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Myndighetsutövning fastställs i svensk rätt genom lag eller annan författning. Uppgifter av allmänt intresse är fastställda i enlighet med svensk rätt om de följer av lag eller annan författning eller av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning.

För *led f* krävs att den rättsliga grunden, dvs. det berättigade intresset, *väger tyngre* än den registrerades intressen och rättigheter. Led *f* gäller inte för behandling som utförs av myndigheter när de fullgör sina uppgifter.

Behandling av personuppgifter får bara ske om alla villkor för tillämpning av minst en av de rättsliga grunder som avses i leden a–f är uppfyllda. Dessutom måste den personuppgiftsansvarige bland annat också se till att principerna i artikel 5 följs.

Personuppgifterna ska enligt artikel 5.1 b samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Att ändamålen ska vara berättigade innebär bland annat, men inte enbart, att de ändamål som den personuppgiftsansvarige är skyldig att ange måste vara berättigade i förhållande till den rättsliga grunden.

Även artikel 6.3 andra stycket innehåller bestämmelser som, i likhet med artikel 5.1 b, kopplar samman de särskilda ändamålen med den rättsliga grunden. Avseende rättslig förpliktelse anges att ändamålen ska vara bestämda i den rättsliga grunden. Vad gäller myndighetsutövning och uppgifter av allmänt intresse anges i stället att ändamålen ska vara nödvändiga för myndighetsutövningen eller för att utföra den fastställda uppgiften av allmänt intresse.

9 Barns samtycke som rättslig grund

9.1 Vårt uppdrag

För att samtycke ska utgöra en rättslig grund för personuppgiftsbehandling vid erbjudande av vissa typer av tjänster direkt till barn under 16 år krävs enligt artikel 8.1 i dataskyddsförordningen vårdnadshavarens samtycke eller dennes godkännande av barnets samtycke. Förordningen tillåter att en lägre åldersgräns föreskrivs i medlemsstaternas nationella rätt. Enligt kommittédirektiven ska vi analysera för- och nackdelar med en lägre åldersgräns.

9.2 Gällande rätt

Det finns i dag ingen uttrycklig reglering vare sig i dataskyddsdirektivet eller i personuppgiftslagen rörande barns samtycke till personuppgiftsbehandling. En bedömning av om den underåriges samtycke ska anses utgöra rättslig grund för personuppgiftsbehandling har därför fått göras från fall till fall.

Datainspektionen har uttalat att det krävs att den som ger samtycket kan förstå innebörden av det. En person som inte själv kan tillgodogöra sig informationen om vad ett samtycke till personuppgiftsbehandling innebär kan inte ge ett rättsligt bindande samtycke.¹

Datainspektionen har vidare ansett att barn under 15 år i allmänhet inte kan anses ha nått en sådan mognad att de kan förstå innebörden av att samtycka till personuppgiftsbehandling. Den bedömningen har

¹ Datainspektionen, Samtycke enligt personuppgiftslagen, Vem kan samtycka? www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/samtycke (hämtad 2017-02-23).

dock rört behandling av barns personuppgifter generellt.² I ett samrådsyttrande som rörde användande av personnummer som spärr för deltagande på en chattsajt har Datainspektionen funnit att föräldrarnas samtycke till barns registrering av sina personuppgifter måste inhämtas i vart fall när det gäller barn som inte fyllt 13 år.³

9.3 Dataskyddsförordningen

9.3.1 Samtycke som rättslig grund för behandling av personuppgifter

I artikel 5 i dataskyddsförordningen finns grundläggande principer som gäller vid all personuppgiftsbehandling. De krav som uppställs i denna artikel ska alltid följas. För att en personuppgiftsbehandling ska vara laglig krävs också att det finns en rättslig grund för behandlingen enligt artikel 6 i dataskyddsförordningen. Samtycke från den registrerade utgör en sådan rättslig grund för personuppgiftsbehandling enligt artikel 6.1 a.

I artikel 4.11 definieras samtycke av den registrerade som varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne. Vad som avses med frivillig, särskild och informerad viljeyttring i artikel 7 a i dataskyddsdirektivet har artikel 29-gruppen uttalat sig om i yttrande 15/2011 om definitionen av begreppet samtycke.⁴ Artikel 29-gruppen arbetar även med att ta fram ett nytt yttrande om begreppet samtycke som förväntas vara klart under det första halvåret 2017.

Samtycke kan lämnas genom en skriftlig eller muntlig förklaring. Det kan innebära att en ruta kryssas i vid besök på en internetsida eller genom val av inställningsalternativ för tjänster på informations-samhällets område. Det kan också ske genom någon annan förklaring

² Datainspektionen, frågor och svar, finns det någon åldersgräns för samtycke, www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/finns-det-nagon-aldersgrans-for-samtycke1/ (hämtad 2017-02-09).

³ Datainspektionens samrådsyttrande i december 2002 med anledning av fråga från ett personuppgiftsombud, se vidare www.datainspektionen.se/personuppgiftsombud/samratsyttrandan/registering-av-personuppgifter-fran-barn-/ (hämtad 2017-03-21).

⁴ Se även artikel 29-gruppens yttrande 2/2013 om appar på smarta enheter, s. 13 f.

eller något annat beteende som i sammanhanget tydligt visar att den registrerade godtar den avsedda behandlingen av sina personuppgifter (se skäl 32 till förordningen).

I artikel 7 i dataskyddsförordningen uppställs vissa villkor för samtycke. Av artikel 7.1 framgår att det är den personuppgiftsansvarige som ska kunna visa att den registrerade har samtyckt till behandling av sina personuppgifter. Enligt artikel 7.2 ska, om den registrerades samtycke lämnas i en skriftlig förklaring som också rör andra frågor, begäran om samtycke läggas fram på ett sätt som klart och tydligt kan särskiljas från de andra frågorna i en begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. I artikel 7.3 anges att de registrerade ska ha rätt att när som helst återkalla sitt samtycke. Det ska vara lika lätt att återkalla som att ge sitt samtycke. Slutligen anges i artikel 7.4 att vid bedömningen av huruvida samtycket är frivilligt ska största hänsyn bland annat tas till huruvida genomförandet av ett avtal, inbegripet tillhandahållandet av en tjänst, har gjorts beroende av samtycke till sådan behandling av personuppgifter som inte är nödvändig för genomförandet av det avtalet.⁵

En förklaring om samtycke som den personuppgiftsansvarige i förväg formulerat bör enligt skäl 42 tillhandahållas i en begriplig och lätt tillgänglig form, med användning av ett klart och tydligt språk och utan oskäligena villkor. För att samtycket ska vara informerat bör den registrerade känna till åtminstone den personuppgiftsansvariges identitet och syftet med den behandling för vilken personuppgifterna är avsedda. Ett samtycke bör inte betraktas som frivilligt om den registrerade inte har någon genuin eller fri valmöjlighet eller om denne inte utan problem kan vägra eller ta tillbaka sitt samtycke.

Om samtycket inte uppfyller de krav som uppställs i förordningen utgör det inte rättslig grund för behandling av personuppgifter. Om syftet med personuppgiftsbehandlingen t.ex. är orimligt eller oproportionerligt har tjänstetillhandahållaren trots användarens samtycke alltså ingen giltig rättslig grund för behandlingen.⁶

⁵ Se även skäl 43.

⁶ Jfr artikel 29-gruppens yttrande 2/2013 om appar på smarta enheter, s. 15.

9.3.2 Personuppgifter som rör barn förtjänar ett särskilt skydd

Att personuppgifter som rör barn anses särskilt skyddsvärda framgår av flera av förordningens bestämmelser och betonas i skälen till förordningen. Det finns dock ingen artikel som anger en specifik ålder för när någon ska anses vara ett barn. Det finns inte heller någon annan enhetlig reglering inom EU som definierar när någon ska anses vara ett barn. Frågan får i stället avgöras genom en tolkning med beaktande av andra rättskällor. Samtliga medlemsstater har ratificerat FN:s konvention om barnets rättigheter, den s.k. barnkonventionen, där barn definieras som varje människa under 18 år, om inte barnet blir myndigt tidigare enligt den lag som gäller barnet (artikel 1).

Som exempel på en bestämmelse i dataskyddsförordningen som särskilt rör barn kan nämnas att barns rätt till integritetsskydd särskilt ska beaktas när personuppgifter behandlas med stöd av den rättsliga grunden i artikel 6.1 f, dvs. när behandlingen bygger på en intresseavvägning.

Vidare föreskrivs i artikel 12.1 att den information som den personuppgiftsansvarige ska lämna enligt artiklarna 13 och 14 ska ges i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, i synnerhet när det gäller information som är särskilt riktad till barn. I skäl 58 anges att det förhållandet att barn förtjänar särskilt skydd, medför att all information och kommunikation som riktar sig till barn bör utformas på ett tydligt och enkelt språk som barnet lätt kan förstå.

Enligt artikel 17.1 f har den registrerade rätt att få sina personuppgifter raderade om de har samlats in med samtycke som rättslig grund i samband med erbjudandet av informationssamhällets tjänster direkt till ett barn i de fall som avses i artikel 8.1 i förordningen. I skäl 65 anges att den registrerades rätt att bli bortglömd är särskilt relevant när den registrerade har gett sitt samtycke som barn, utan att vara fullständigt medveten om riskerna med behandlingen, och senare vill ta bort dessa personuppgifter, särskilt på internet. Den registrerade bör kunna utöva denna rätt även när han eller hon inte längre är barn.

Tillsynsmyndigheten ska också ägna särskild uppmärksamhet åt insatser som riktar sig till barn, när den enligt artikel 57.1 b utför sin uppgift att öka allmänhetens medvetenhet om och förståelse för

risker, regler, skyddsåtgärder och rättigheter i fråga om behandling av personuppgifter.

I skäl 38 uttalas att barns personuppgifter förtjänar ett särskilt skydd, eftersom barn kan vara mindre medvetna om risker, skyddsåtgärder och rättigheter. Det särskilda skyddet bör i synnerhet gälla användningen av barns personuppgifter i marknadsföringssyfte, för att skapa personlighets- eller användarprofiler samt för insamling av uppgifter när tjänster som erbjuds direkt till barn utnyttjas. Samtycke från den person som har föräldraansvar över ett barn bör enligt uttalandet inte krävas för förebyggande eller rådgivande tjänster som erbjuds direkt till barn.

I skäl 71 till förordningen anges att barns personuppgifter inte bör användas för automatiserat beslutsfattande i form av bland annat profilering. Med profilering avses enligt samma skäl och artikel 4.4 i förordningen automatisk behandling av personuppgifter med bedömning av personliga aspekter rörande en fysisk person, särskilt för att analysera eller förutse aspekter avseende den registrerades arbetsprestation, ekonomiska situation, hälsa, personliga preferenser eller intressen, pålitlighet eller beteende, vistelseort eller förflyttningar.

9.3.3 Barns samtycke

I artikel 8.1 i dataskyddsförordningen anges att vid erbjudande av informationssamhällets tjänster direkt till ett barn, ska behandling av personuppgifter som rör ett barn få ske med stöd av artikel 6.1 a om barnet är minst 16 år. Om barnet är under 16 år ska sådan behandling vara tillåten endast om och i den mån samtycket ges eller godkänns av den person som har föräldraansvar för barnet. Medlemsstaterna får föreskriva en lägre ålder i sin nationella rätt, under förutsättning att denna ålder inte är lägre än 13 år. Bestämmelsen omfattar givetvis endast situationer när personuppgifter behandlas. Om en tjänst tillhandahålls utan att personuppgifter behandlas faller den utanför förordningens tillämpningsområde.

I artikel 8.2 anges att den personuppgiftsansvarige ska göra rimliga ansträngningar för att kontrollera att samtycket ges eller godkänns av den person som har föräldraansvar för barnet, med hänsyn tagen till tillgänglig teknik. Slutligen anges i artikel 8.3 att punkt 1 i artikeln inte ska påverka tillämpningen av allmän avtalsrätt i medlemsstaterna,

såsom bestämmelser om giltigheten, upprättandet eller effekten av ett avtal som gäller ett barn.

Det bör noteras att artikel 8.1 endast hänvisar till artikel 6 och inte till artikel 9. Vid vilken ålder barn kan samtycka till behandling av känsliga personuppgifter framgår alltså inte av förordningen och omfattas inte heller av våra överväganden. Det bör också poängteras att bestämmelsen endast är tillämplig när den rättsliga grunden för personuppgiftsbehandlingen är samtycke och inte när det finns en annan rättslig grund för behandlingen, såsom exempelvis avtal enligt artikel 6.1 b.

9.4 Utgångspunkter för vår bedömning

9.4.1 Inledning

Det vi har att ta ställning till är vid vilken ålder ett barn bör kunna samtycka till viss behandling av barnets personuppgifter utan föräldrarnas medgivande. Det förtjänar emellertid redan här att noteras att även i det fall samtycke får inhämtas från ett barn, så kräver data-skyddsförordningen att tjänstetillhandahållaren beaktar barnets begränsade förståelse för behandlingen av personuppgifter. På grund av förordningens särskilda fokus på barns sårbarhet bör dessutom principerna om uppgiftsminimering och ändamålsbegränsning i artikel 5 tillämpas strikt.⁷ En personuppgiftsbehandling kan alltså på grund av de övriga bestämmelserna i förordningen vara otillåten, trots att samtycke har lämnats av ett barn som har uppnått den i svensk rätt satta åldersgränsen.

9.4.2 Barnets bästa och barnets rätt till integritet

Vid bedömningen av vid vilken ålder ett barn själv bör få samtycka till att dess personuppgifter behandlas måste bestämmelserna i FN:s barnkonvention beaktas. Som nämnts ovan avses med barn i konventionens mening varje människa under 18 år, om inte barnet blir myndigt tidigare enligt den lag som gäller barnet. I artikel 3 i konventionen fastslås att barnets bästa ska komma i främsta rummet vid alla

⁷ Jfr artikel 29-gruppens yttrande 2/2013 om appar på smarta enheter, s. 25.

åtgärder som rör barn, vare sig de vidtas av offentliga eller privata sociala välfärdsinstitutioner, domstolar, administrativa myndigheter eller lagstiftande organ.

Barnkonventionen syftar till att ge barn, oavsett bakgrund, rätt att behandlas med respekt och att få komma till tals. I artikel 12 anges bland annat att konventionsstaterna ska tillförsäkra det barn som är i stånd att bilda egna åsikter rätten att fritt uttrycka dessa i alla frågor som rör barnet, varvid barnets åsikter ska tillmätas betydelse i förhållande till barnets ålder och mognad. Artikel 13 slår fast att barnet har rätt till yttrandefrihet. Denna rätt innefattar frihet att oberoende av territoriella gränser söka, motta och sprida information och tankar av alla slag, i tal, skrift eller tryck, i konstnärlig form eller genom annat uttrycksmedel som barnet väljer.

Samtidigt som barnet har rätt till yttrande- och informationsfrihet behöver det finnas ett skydd för barnet när dess personuppgifter behandlas. Det ska ske med beaktande bland annat av bestämmelsen om föräldrars ledning i artikel 5 i barnkonventionen. Bestämmelsen ger föräldrar och andra vårdnadshavare rättigheter och skyldigheter att ge barnet lämplig ledning och råd vid utövandet av barnets rättigheter. Vägledning ska ges på ett sätt som överensstämmer med barnets fortlöpande utveckling. Barnet ska alltså med stigande ålder få större möjlighet att själv styra över på vilket sätt det vill ta vara på sina rättigheter. Eftersom barnet är en person som håller på att utvecklas fysiskt och psykiskt, måste utövandet av barnets rättigheter anpassas till dess utvecklingsnivå.

Det måste alltså göras en avvägning mellan barnets behov av skydd och dess rätt till informationsfrihet. Ju äldre barnet blir, desto mindre blir dess behov av skydd och desto större tyngd ska tillmätas rätten till yttrande- och informationsfrihet.

Vid avvägningen måste också hänsyn tas till barnets rätt till integritet. Artikel 16 stadgar att inget barn får utsättas för godtyckliga eller olagliga ingripanden i sitt privat- eller familjeliv, sitt hem eller sin korrespondens och inte heller för olagliga angrepp på sin heder och sitt anseende. Detta måste respekteras av alla, även av barnets vårdnadshavare. Barnets rätt till integritet måste således balanseras mot föräldrarnas skyldighet och rättighet att genom insyn i barnets förehavanden tillvarata barnets intressen och se till barnets bästa.

9.4.3 När är artikel 8.1 i dataskyddsförordningen tillämplig?

För att kunna bedöma vid vilken ålder barn kan tänkas uppnå en tillräcklig mognad och insikt i fråga om personuppgiftsbehandling finns det anledning att närmare analysera innebörden av artikel 8.

Erbjudande av informationssamhällets tjänster

Det är enligt dataskyddsförordningen endast vid erbjudande av informationssamhällets tjänster till någon som är under 16 år som samtycket till behandlingen behöver ges eller godkännas av den som har föräldraansvaret för barnet. När det gäller personuppgiftsbehandling som inte sker i samband med att informationssamhällets tjänster erbjuds får en bedömning, liksom tidigare, göras i varje enskilt fall av den registrerades förmåga att förstå innebörden av ett lämnat samtycke.

Begreppet informationssamhällets tjänster definieras i artikel 4.25 i dataskyddsförordningen som alla tjänster enligt definitionen i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535⁸. I sistnämnda artikel anges att informationssamhällets tjänster är tjänster som vanligtvis utförs mot ersättning, på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare. I denna definition avses med på distans att tjänsten tillhandahålls utan att parterna är närvarande samtidigt. Med på elektronisk väg avses att tjänsten sänds vid utgångspunkten och tas emot vid slutpunkten med hjälp av utrustning för elektronisk behandling och lagring av uppgifter och som i sin helhet sänds, befordras och tas emot genom tråd, radio, optiska medel eller andra elektromagnetiska medel. Med på individuell begäran av en tjänstemottagare avses att tjänsten tillhandahålls genom överföring av uppgifter på individuell begäran.

Informationssamhällets tjänster är ett EU-rättsligt begrepp som även används i bland annat e-handelsdirektivet⁹. I ingressen till detta

⁸ Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster.

⁹ Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden ("Direktiv om elektronisk handel").

direktiv hänvisas till definitionen av begreppet i direktiv 98/34/EG¹⁰, som nu har kodifierats och ersatts av ovan nämnda direktiv (EU) 2015/1535. Ledning för tolkningen av begreppet informationssamhällets tjänster bör därför kunna hämtas från e-handelsdirektivet och den tolkning av detta som gjorts av EU-domstolen.

I skäl 18 till e-handelsdirektivet anges följande. Informationssamhällets tjänster omfattar en mängd näringsverksamheter som bedrivs online. Dessa verksamheter kan särskilt bestå i försäljning av varor online. Själva leveransen av varor eller tillhandahållandet av offline-tjänster omfattas inte. Informationssamhällets tjänster begränsas inte till enbart tjänster som föranleder avtal online utan gäller även tjänster, i den mån de utgör näringsverksamhet, som inte betalas av de som mottar dem, exempelvis tillhandahållande av information eller kommersiella meddelanden online eller tillhandahållande av sökmöjligheter samt åtkomst till och hämtning av data.

Vid tolkningen av begreppet informationssamhällets tjänster i e-handelsdirektivet har EU-domstolen konstaterat att det inte krävs att tjänsten betalas av den som åtnjuter tjänsten för att den ska omfattas av definitionen. Tjänsten kan t.ex. finansieras genom inkomster via reklam som visas på en webbplats.¹¹

När e-handelsdirektivet genomfördes i svensk rätt uttalade regeringen att med informationssamhällets tjänster avses – förenklat uttryckt – varje aktivitet som sker online, med någon ekonomisk innebörd. Regeringen menade att begreppet omfattar en mängd olika tjänster, däribland informationstjänster och söktjänster.¹² Artikel 29-gruppen har uttalat att i rättsligt avseende ingår sociala nätverk, sökmotorer och appar i begreppet informationssamhällets tjänster.¹³

Mot bakgrund av ovanstående kan enligt vår bedömning begreppet informationssamhällets tjänster innefatta bland annat olika sociala medier, såsom till exempel bloggar, internetforum, webbplatser för videoklipp, chattprogram och sociala nätverk. Även onlinespel och

¹⁰ Europaparlamentets och rådets direktiv 98/34/EG av den 22 juni 1998 om ett informationsförfarande beträffande tekniska standarder och föreskrifter och beträffande föreskrifter för informationssamhällets tjänster.

¹¹ Se dom *Papasavvas*, C-291/13, EU:C:2014:2209, punkterna 28–30 och dom *Bond van Adverteerders m.fl.*, 352/85, EU:C:1988:196, punkt 16.

¹² Prop. 2001/02:150 s. 1 och 19.

¹³ Se artikel 29-gruppens yttrande 5/2009 om sociala nätverk på Internet, s. 4 f., artikel 29-gruppens yttrande 1/2008 om dataskyddsfrågor med anknytning till sökmotorer, s. 5 och not 6 och 7 på samma sida, samt artikel 29-gruppens yttrande 2/2013 om appar på smarta enheter, s. 24 not 46.

olika applikationer (appar) med spel eller annat innehåll kan omfattas av definitionen.

*Behandling av personuppgifter inom ramen
för informationssamhällets tjänster*

Det är inte nödvändigt att behandla personuppgifter i samband med erbjudande av informationssamhällets tjänster. I praktiken är det emellertid mycket vanligt att behandling av personuppgifter utgör ett villkor för tillhandahållande av sådana tjänster.

Vilka personuppgifter som samlas in, hur de används av tjänestetillhandahållaren själv och hur dessa uppgifter delas med andra varierar från tjänst till tjänst. Tjänestetillhandahållarna har ibland ett intresse av att samla in så många personuppgifter som möjligt, eftersom de kan ha ett stort ekonomiskt värde.

De uppgifter som samlas in kan vara uppgifter som den enskilde måste lämna ifrån sig för att få använda en tjänst, såsom ett namn, användarnamn, födelsedatum, kön, adress, e-postadress och mobiltelefonnummer. Det kan även vara uppgifter om kreditkorts- och betalningsinformation.

Ofta behandlas också uppgifter vid användningen av en tjänst. Det kan bland annat röra sig om geografiska lokaliseringssuppgifter eller vem användaren interagerar med. Även webbläsarhistorik kan tillskapas och kan bli föremål för senare behandling. Uppgifter kan också synkroniseras med andra användares uppgifter, exempelvis uppgifter från adressboken på en telefon.

Uppgifterna kan användas i olika syften av tillhandahållaren av tjänsten, t.ex. för direktmarknadsföring. Det kan ske på olika sätt. Med s.k. beteendebaserad marknadsföring menas förenklat att användare spåras när de surfar på internet och att det med tiden byggs upp profiler som sedan används för att förse användarna med reklam som passar deras intressen.¹⁴ Personuppgifterna tillhandahålls ofta även till andra än den som tillhandahåller tjänsten, t.ex. i marknadsförings- syfte.

¹⁴ Jfr artikel 29-gruppens yttrande 2/2010 om beteendebaserad reklam på internet, s. 3 och 5.

Direkt till barn

Det framgår inte av dataskyddsförordningen vad som avses med uttrycket att en tjänst ska erbjudas *direkt till barn*. Begreppet skulle kunna tolkas på flera olika sätt.

En möjlig tolkning av begreppet är att det endast omfattar tjänster som uttryckligen riktar sig till barn. Ett problem med denna tolkning är att det i dag inte finns något krav på att tjänstetillhandahållarna ska ange vilken ålder de anser är lämplig för användning av en tjänst. Inte heller finns det någon standard som anger vilka kriterier som ska vara uppfyllda för en viss åldersgräns. Ytterligare problem som skulle kunna uppstå med denna tolkning är att en tjänstetillhandahållare skulle kunna kringgå den aktuella bestämmelsen genom att ange att tjänsten endast riktar sig till personer som inte är barn.

En annan möjlig tolkning är att det är användarens faktiska ålder som avgör om tjänsten omfattas av begreppet. Det skulle innebära att den som tillhandahåller en tjänst och hanterar personuppgifter med stöd av samtycke i samtliga fall måste veta om den som använder tjänsten är ett barn eller inte. Alla tjänstetillhandahållare som hanterar personuppgifter skulle i sådant fall behöva kontrollera åldern på alla personer som använder tjänsten. Det kan starkt ifrågasättas om det skydd som kan uppnås motiverar att personuppgifter om ålder samlas in från samtliga användare.

En tredje möjlig tolkning är att artikel 8.1 i dataskyddsförordningen tar sikte på sådana tjänster som kan antas användas av barn. Bedömningen blir då inte beroende av hur tjänsteleverantören presenterar sin tjänst utåt. Både tjänster som direkt marknadsförs mot barn och tjänster som i och för sig inte marknadsförs som särskilt anpassade för barn, men som på grund av sin utformning eller sitt innehåll och funktion är av det slaget att de typiskt sett kan antas användas av barn, omfattas vid en sådan tolkning av bestämmelsen. Det finns enligt vår mening mycket som talar för denna tolkning.

Begreppet är emellertid EU-rättsligt och det är EU-domstolen som ytterst kan ge vägledning för tolkningen. Artikel 29-gruppen arbetar för närvarande med att ta fram ett yttrande om gruppens syn på innebörden av begreppet samtycke. Yttrandet, som planeras vara klart under det första halvåret 2017, förväntas innehålla klagörande uttalanden även rörande barns samtycke och de olika rekvisiten i

artikel 8. Viss vägledning för tolkningen av begreppet bör därför kunna finnas till hands när förordningen ska börja tillämpas.

Föräldraansvaret

Det är den som har föräldraansvaret för barnet som enligt artikel 8.1 i dataskyddsförordningen ska samtycka till personuppgiftsbehandlingen eller godkänna barnets samtycke. Vad som avses med föräldraansvar framgår dock inte av förordningen.

I artikel 1.2 i 1996 års Haagkonvention¹⁵ anges att begreppet föräldraansvar i konventionen omfattar vårdnad eller varje liknande förhållande som avgör föräldrars, förmyndares eller andra rättsliga företrädares rättigheter, befogenheter och ansvar i förhållande till barnets person eller egendom. I artikel 2.7 i Bryssel II-förordningen¹⁶ definieras föräldraansvar som alla rättigheter och skyldigheter som en fysisk eller juridisk person har tillerkänts genom en dom, på grund av lag eller genom en överenskommelse med rättslig verkan, med avseende på ett barn eller dess egendom. Föräldraansvar omfattar bland annat vårdnad och umgänge.

I Sverige regleras föräldraansvaret främst i föräldrabalken. Vårdnadshavarna har enligt föräldrabalken rätt, och skyldighet, att bestämma i frågor som rör barnets personliga angelägenheter. Vårdnadshavaren ska i takt med barnets stigande ålder och utveckling ta allt större hänsyn till barnets synpunkter och önskemål (6 kap. 11 § föräldrabalken). Barn står som regel under vårdnad av båda sina föräldrar eller en av dem om rätten har anförtrott vårdnaden åt en eller två särskilt förordnade vårdnadshavare. Den som har vårdnaden om ett barn har ett ansvar för barnets personliga förhållanden och ska se till att barnens behov av omvårdnad, trygghet och god fostran blir tillgodosedda. Barnets vårdnadshavare svarar även för att barnet får den tillsyn som behövs med hänsyn till dess ålder, utveckling och övriga

¹⁵ Den i Haag den 19 oktober 1996 dagtecknade konventionen om behörighet, tillämplig lag, erkännande, verkställighet och samarbete i frågor om föräldraansvar och åtgärder till skydd för barn. Artiklarna 1–53 i konventionen gäller i originaltexternas lydelse som lag här i landet, jfr 1 § lagen (2012:318) om 1996 års Haagkonvention.

¹⁶ Rådets förordning (EG) nr 2201/2003 av den 27 november 2003 om domstols behörighet och om erkännande och verkställighet av domar i äktenskapsmål och mål om föräldraansvar samt om upphävande av förordning (EG) nr 1347/2000.

omständigheter (6 kap. 1 och 2 §§ föräldrabalken). Vårdnaden om ett barn består till dess att barnet fyllt 18 år.

Artikel 29-gruppen har i ett yttrande påtalat att vårdnadshavarnas ställning inte har någon absolut eller ovillkorlig prioritet över barnets. Principen om att barnets bästa ska komma i främsta rummet kan ibland, enligt artikel 29-gruppen, ge barnet rättigheter som går före vårdnadshavarnas önskemål. Kravet på att barnet ska företrädas av personer som enligt lag har rätt att företräda det påverkar inte det förhållandet att barnet från och med en viss ålder ska ges möjlighet att höras i frågor som berör det.¹⁷

Vårdnadshavarna får emellertid inte heller lämna ifrån sig sitt ansvar för barnet genom att låta det själv bestämma i en omfattning som det inte är moget för. Vårdnadshavarna är skyldiga att ingripa om barnet kan komma till skada eller det visar sig inte vara moget för att själv fatta beslut.¹⁸

9.4.4 Något om olika åldersgränser i svensk lagstiftning

En person under 18 år är omyndig och får som huvudregel inte själv råda över sin egendom eller åta sig förbindelser (9 kap. 1 § föräldrabalken). Detta innebär dock inte att ett avtal som ett barn har ingått per automatik blir ogiltigt. Om ett barn företar en rättshandling som han eller hon inte får företa, är rättshandlingen ogiltig bara om den är ofördelaktig för barnet. Om vårdnadshavare eller förmyndare godkänner avtalet är det ändå giltigt. Godkännandet behöver inte vara uttryckligt, utan kan vara ett så kallat tyst godkännande.¹⁹

Det finns dock ett antal undantag från ovan nämnda huvudregel. I vissa sammanhang får barnet självt ingå rättshandlingar och föra sin talan. Dessutom ska ibland barnets samtycke ges avgörande betydelse. I flera författningar har även föreskrivits att barnets vilja ska tillmätas betydelse med ökad ålder och mognad.

Enligt 21 kap. 5 § föräldrabalken gäller att i det fall barnet har nått en sådan ålder och mognad att dess vilja bör beaktas, får verkställighet

¹⁷ Artikel 29-gruppens yttrande 2/2009 om skydd för uppgifter om barn (Allmänna riktlinjer och specialfallet skolor), s. 4 f.

¹⁸ Jfr Walin och Vängby, Föräldrabalken (20 maj 2016, Zeteo), kommentaren till 6 kap. 11 § föräldrabalken, och prop. 1981/82:168.

¹⁹ Jfr Walin och Vängby, Föräldrabalken, (20 maj 2016, Zeteo), kommentaren till 9 kap. 1 § föräldrabalken.

av t.ex. en dom om vårdnad inte ske mot barnets vilja, utom då rätten finner det nödvändigt av hänsyn till barnets bästa.

Inom den frivilliga hälso- och sjukvården krävs enligt 4 kap. 2 § patientlagen (2014:821) som huvudregel patientens samtycke till vården. Det är vårdgivaren som har att avgöra om ett giltigt samtycke har getts.²⁰ När patienten är ett barn ska barnets inställning till den aktuella vården eller behandlingen så långt som möjligt klarläggas. Barnets inställning ska tillmätas betydelse i förhållande till hans eller hennes ålder och mognad (4 kap. 3 §). Krav på ålder och mognadsgrad kan variera beroende på om frågan gäller t.ex. preventivmedelsrådgivning eller allvarlig sjukdom. Olika mognadsgrad kan krävas för olika former av beslut.²¹

I Sverige har ofta åldersgränsen för barns samtycke och möjlighet att själva agera i rättsliga och andra sammanhang satts vid 15 år. När det gäller forskning som avser människor ska forskningspersonen själv informeras om och samtycka till forskningen, om han eller hon har fyllt 15 år men inte 18 år och inser vad forskningen innebär för hans eller hennes del (18 § lagen om etikprövning av forskning som avser människor).

Barn som har fyllt 15 år har rätt att själv föra sin talan i mål och ärenden enligt socialtjänstlagen (2001:453), lagen (1990:52) med särskilda bestämmelser om vård av unga och lagen (1991:1128) om psykiatrisk tvångsvård. Enligt sistnämnda lag bör även en patient som är yngre än 15 år höras, om det kan vara till nytta för utredningen och det kan antas att patienten inte tar skada av att höras. En underårig kan inte dömas till påföljd för brott som han eller hon begått innan det att han eller hon har fyllt 15 år (1 kap. 6 § brottsbalken). Dessutom är sexuellt umgänge med barn kriminaliserat såvitt gäller barn under 15 år (6 kap. 4 § brottsbalken). 15 år är alltså en vedertagen åldersgräns som har ansetts vara väl avvägd i många sammanhang.²²

När det gäller barnets möjligheter att ingå avtal och andra angelägenheter av ekonomisk natur har åldern i svensk rätt ofta satts vid 16 år. Barn får således från det att de fyllt 16 år själva råda över in-

²⁰ Rynning, Samtycke till medicinsk vård och behandling, 1994 s. 286 f. och prop. 2002/03:50 s. 135.

²¹ Rynning, Samtycke till medicinsk vård och behandling, 1994 s. 286 f., prop. 2002/03:50 s. 135, och Socialstyrelsens meddelandeblad nr.7/2010 om barn under 18 år som söker hälso- och sjukvård.

²² Se t.ex. prop. 2002/03:50 s. 136.

komster de tjänat (9 kap. 3 § föräldrabalken) och driva rörelse om föräldrarna godkänt detta (13 kap. 13 §). Barn får själva ingå avtal om anställning eller annat arbete, men endast om vårdnadshavaren samtycker till avtalet. Barnet får självt säga upp avtalet och, om barnet har fyllt 16 år, utan nytt samtycke avtala om annat arbete av liknande art (6 kap. 12 §).

I svensk lag är det ovanligt att det stipuleras en lägre åldersgräns än 15 år, men när det gäller adoption stadgas att den som har fyllt 12 år som huvudregel inte får adopteras utan eget samtycke (4 kap. 5 § föräldrabalken).

9.4.5 Direktreklam till barn

Personuppgifter kan som ovan angetts användas i syfte att rikta direktreklam till användaren när informationssamhällets tjänster utnyttjas. Direktmarknadsföring är ofta ett grundläggande inslag i affärsmodellen för bland annat sociala nätverkstjänster.²³

Enligt 5 § marknadsföringslagen (2008:486) ska marknadsföring stämma överens med god marknadsföringssed. Marknadsföring som strider mot god marknadsföringssed är enligt 6 § marknadsföringslagen att anse som otillbörlig om den i märkbar mån påverkar eller sannolikt påverkar mottagarens förmåga att fatta ett välgrundat affärsbeslut.

Med god marknadsföringssed förstås god affärssed eller andra vedertagna normer som syftar till att skydda konsumenter och näringsidkare vid marknadsföring av produkter (3 §). Hit hör även det normsystem som har utvecklats inom näringslivet, främst Internationella handelskammarens (ICC) grundregler för reklam, men även andra uppförande- och branschkode. Förutom god affärssed och god yrkessed innefattar begreppet god marknadsföringssed även andra vedertagna normer för marknadsföring. Därmed avses bland annat speciallagstiftning, Konsumentverkets föreskrifter och allmänna råd, de normer som Marknadsdomstolen har skapat genom sin praxis samt andra internationella vedertagna normer inom ramen för lagens syfte.²⁴

²³ Jfr artikel 29-gruppens yttrande 5/2009 om sociala nätverk på Internet, s. 10.

²⁴ Prop. 2007/08:115 s. 69 f.

Marknadsdomstolen har bedömt att det som huvudregel inte är tillåtet att rikta direktreklam till barn under 16 år eftersom detta anses strida mot god marknadsföringssed. Undantag kan finnas med hänsyn till omständigheterna i det enskilda fallet, t.ex. när vårdnadshavarens samtycke finns. Domstolen har även bedömt att sådan reklam kan vara otillbörlig enligt 6 § marknadsföringslagen. Inte heller får köpuppsmaningar, enligt Marknadsdomstolen, riktas direkt till barn, dvs. någon under 18 år, eftersom detta kan anses utgöra sådan aggressiv marknadsföring som enligt 7 § marknadsföringslagen inte får användas.²⁵

Det finns en svensk branschöverenskommelse om direktmarknadsföring som har granskats av Datainspektionen.²⁶ I branschöverenskommelsen anges bland annat att direktmarknadsföring normalt inte får riktas till barn, såvida det inte finns en anknytning mellan den minderåriga och marknadsföraren där sådana kontakter kan sägas vara förutsatta av omständigheterna. Sådan anknytning kan vara kundförhållande, medlemskap eller liknande.

9.4.6 Yttranden till utredningen angående åldersgränsen

Barnombudsmannen har i ett yttrande till utredningen ansett att åldersgränsen bör vara 15 år och uttalat följande. Hänsyn måste tas till såväl barnets rätt till delaktighet och information som till barnets rätt till skydd. År 2014 hade FN:s kommitté för barnens rättigheter en diskussion om digitala medier och barns rättigheter. Där framhövs hur digitala medier ger barn stora möjligheter att lära, delta, spela arbeta och umgås, men samtidigt ställs barn inför nya risker. Därför måste det finnas en balans mellan barnets självbestämmande och skydd av barn online/på nätet. Huvudfokus bör vara förebyggande arbete och att stärka barns kunskaper och förmåga. Först då kan barnet delta fullt ut i samhället och göra sin röst hörd på ett säkert sätt online/på nätet. Det är av stor vikt att barnet kan förutse de konsekvenser som en behandling av personuppgifter kan medföra. En 15-årsgräns – som är en vanligt förekommande åldersgräns i

²⁵ Se MD 2012:14 och MD 1999:26.

²⁶ SWEDMA:s regler för användningen av personuppgifter m.m. vid direktmarknadsföring för försäljnings-, insamlings- medlemsvärningsändamål och liknande samt Datainspektionens yttrande den 16 juni 1999, dnr 1338-99.

Sverige – innebär att barn och unga fortfarande har möjlighet att delta i olika sociala medier med vårdnadshavarens samtycke.

Även Statens medieråd har lämnat ett yttrande till utredningen. Medierådet är kritiskt till bestämmelsen i artikel 8.1 i dataskyddsförordningen och anför följande. Det finns i nuläget inte några fungerande metoder för säker åldersverifiering. Den som vill kan enkelt kringgå bestämmelsen i artikel 8.1. Förslaget om vårdnadshavarens samtycke blir mot denna bakgrund ett slag i luften. Om metoder för åldersverifiering kommer att skapas så kommer det per definition att leda till att tjänsteleverantören inte får tillgång till färre personuppgifter, utan fler. Föräldrar kommer vidare att tvingas välja mellan att helt neka barnet åtkomst till de digitala tjänsterna eller godkänna ett svårbegripligt avtal som dessutom kan vara skrivet på ett sätt så att det främjar företagets intresse av datainsamling. Mot denna bakgrund bör gränsen för krav på föräldrars samtycke sättas vid en så låg ålder som möjligt, dvs. 13 år.

9.5 Överväganden och förslag

Utredningens förslag: Barn som har fyllt 13 år ska själva kunna samtycka till personuppgiftsbehandling i samband med att informationssamhällets tjänster erbjuds direkt till barn.

Inledning

Det finns inget givet svar på frågan vid vilken ålder ett barn själv bör kunna samtycka till att dess personuppgifter behandlas vid erbjudandet av informationssamhällets tjänster. Det är dessutom, som framgår av avsnitt 9.4.3, fortfarande oklart vilka situationer som kommer att träffas av bestämmelsen i artikel 8.1. Svårigheterna med att sätta en åldersgräns följer också av det faktum att tjänsternas utformning varierar och ständigt utvecklas, även avseende den behandling av personuppgifter som sker inom ramen för sådana tjänster. Dataskyddsförordningen ger dock inget utrymme för en differentierad åldersgräns eller en situations- eller individanpassad bedömning. Den fråga som vi har att ta ställning till är om åldersgränsen ska vara 16 år eller om den ska vara lägre än så, dock lägst 13 år.

Det finns inte någon sedan tidigare lagreglerad åldersgräns inom detta område att jämföra med, vare sig på EU-nivå eller i svensk rätt. Inte heller finns det något närliggande rättsområde som direkt skulle kunna användas som förebild. Det finns däremot andra länder där det har fastställts en åldersgräns för när ett giltigt samtycke till behandling av personuppgifter kan ges. Som exempel kan nämnas USA, där gränsen är 13 år.²⁷

I kommissionens förslag till dataskyddsförordning den 25 januari 2012 var åldersgränsen satt till 13 år.²⁸ Även Europaparlamentets lagstiftningsresolution den 12 mars 2014 utgick från åldersgränsen 13 år.²⁹ Europeiska datatillsynsmannen har också ansett att åldersgränsen borde vara 13 år.³⁰ I Rådets generella ståndpunkt inför den så kallade trepartsdialogen med parlamentet och kommissionen angavs däremot ingen åldersgräns alls. Rådets ståndpunkt var i stället att det endast skulle vara tillåtet att behandla personuppgifter som rör ett barn om och i den mån sådant samtycke ges eller godkänns av den person som har föräldraansvar över barnet eller ges av barnet självt i situationer där det enligt unionslagstiftningen eller medlemsstaternas lagstiftning behandlas som giltigt.³¹

Först i ett sent skede av trepartsdialogen kom parterna överens om att höja åldersgränsen i artikel 8.1 till 16 år, med en möjlighet för medlemsstaterna att i nationell rätt sänka åldersgränsen till 13 år. Såvitt vi har kunna utröna föregicks denna ändring inte av någon egentlig diskussion i breda kretsar. Vi har därmed inte heller kunna finna någon dokumentation rörande vilka motiv som låg bakom höjningen till 16 år.

²⁷ Jfr Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505.

²⁸ Förslag till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning) (COM[2012] 11 final av den 25 januari 2012).

²⁹ Europaparlamentets lagstiftningsresolution av den 12 mars 2014 om kommissionens förslag enligt föregående fotnot.

³⁰ Se bilaga till yttrande 3/2015, Europas stora möjlighet, Europeiska datatillsynsmannens rekommendationer om EU:s alternativ för reform av uppgiftsskyddet, s. 13.

³¹ Rådets dokument 9565/15.

Harmonisering som skäl

Dataskyddsförordningen syftar till att harmonisera regelverken rörande personuppgiftsbehandling inom EU. Det kan tyckas anmärkningsvärt att medlemsstaterna just när det gäller barns samtycke ges frihet att avvika i så stor utsträckning som förordningen öppnar för. Åldersgränsen kan sättas vid 16, 15, 14 eller 13 år. Vi är tveksamma till att en stor variation på detta område gynnar skyddet för barnens integritet. Dessutom blir regelverken svårare för tjänstetillhandahållarna att tillämpa om staternas lagstiftning föreskriver olika åldersgränser. Det finns emellertid, innan vi lämnar vårt betänkande, ingen möjlighet att förutse hur frekvent det kommer att bli att medlemsstaterna väljer att använda det utrymme att sänka åldersgränsen som ges i bestämmelsen i artikel 8.1 i förordningen. Även om vi i Sverige skulle välja att behålla den i förordningen satta åldersgränsen, för att så långt som möjligt försöka uppnå en harmonisering, är det alltså i nuläget långt ifrån säkert att detta skulle bli effekten. Detta är således inte i sig ett tungt vägande skäl för att behålla den i förordningen föreskrivna 16-årsgränsen.

Risker och skyddsmekanismer

Integritetskommittén har haft i uppdrag att utifrån ett individperspektiv kartlägga och analysera sådana faktiska och potentiella risker för intrång i den personliga integriteten som kan finnas i samband med användning av informationsteknik (dir. 2014:65). Kommittén bedömde att användningen av vissa sociala medier innebär en allvarlig risk för den personliga integriteten, bland annat eftersom det i praktiken är omöjligt för användare att avgöra för vilka ändamål uppgifterna som samlas in kommer att användas. Kommittén pekade bland annat på riskerna för att uppgifterna sprids vidare till andra företag men också på att omfattande uppgifter om användarna riskerar att komma underrättelsetjänster i tredje länder till del.³²

Integritetsriskerna för barn som använder informationssamhällets tjänster är i första hand kopplade till att ett samtycke i de flesta fall innebär att en stor mängd uppgifter om barnet kan lagras och spridas i marknadsföringssyfte. Direktmarknadsföring är ofta ett grundlägg-

³² SOU 2016:41 s. 395 f.

gande inslag i affärsmodellen för sociala nätverkstjänster och andra typer av informationssamhällets tjänster.³³ Användarnas personuppgifter samlas in och sparas, bland annat för att beteendebaserad reklam ska kunna riktas till var och en. Detta kan betraktas som en slags kartläggning av användarnas personliga förhållanden, i den mån de kommer till uttryck i deras aktiviteter online, t.ex. vid användning av en söktjänst eller ett socialt media. En sådan kartläggning kan, särskilt om den pågår under lång tid, i sig medföra stora risker för intrång i den personliga integriteten.

Att förstå i vilken utsträckning och för vilket syfte personuppgifter behandlas i samband med att en tjänst erbjuds och används kräver en hög grad av insikt och mognad. Vilka personuppgifter som behandlas och hur dessa sedermera kommer att användas av tjänsteleverantören och andra parter är svårt för tjänsteleverantören att beskriva på ett enkelt och begripligt sätt. Det är som regel komplex och svår information att ta till sig även för en vuxen. Det är också svårt att utifrån den information som ges förstå och värdera riskerna med personuppgiftsbehandlingen. Det finns dessutom en risk att yngre barn, för att inte bli utanför den sociala gemenskapen, samtycker till en mycket omfattande personuppgiftsbehandling utan att förstå innebörden av ett sådant beslut.

När det gäller riskerna kopplade till marknadsföring har artikel 29-gruppen ansett att personuppgiftsansvariga särskilt bör avhålla sig från att behandla barns uppgifter för ändamål som direkt eller indirekt rör beteendebaserad marknadsföring, eftersom detta skulle ligga utanför ett barns begreppsram och därför överskrida gränsen för laglig uppgiftsbehandling.³⁴ I skäl 38 till dataskyddsförordningen anges vidare att skydd för barns personuppgifter i synnerhet bör gälla när uppgifterna används i marknadsföringssyfte, när personlighets- och användarprofiler skapas samt när personuppgifter om barn samlas in då tjänster som erbjuds direkt till barn utnyttjas. Det finns också olika branschöverenskommelser som syftar till att hindra att barns personuppgifter används i marknadsföringssyfte. Enligt svensk rätt strider det även som huvudregel mot god marknadsföringssed att rikta direktreklam till barn under 16 år.

³³ Artikel 29-gruppens yttrande 5/2009 om sociala nätverk på Internet, s. 10, och artikel 29-gruppens yttrande 1/2008 om dataskyddsfrågor med anknytning till sökmotorer.

³⁴ Artikel 29-gruppens yttrande 2/2013 om appar på smarta enheter, s. 25.

När det gäller barns begränsade förmåga att förstå konsekvenserna av ett samtycke innehåller dataskyddsförordningen som nämnts tidigare ett antal bestämmelser och skäl som särskilt syftar till att värna barns intressen vid personuppgiftsbehandling. Artikel 12.1 och skäl 58 ger uttryck för att information och kommunikation som riktar sig till barn ska utformas på ett tydligt och enkelt språk som barnet lätt kan förstå. Av definitionen i artikel 4.11 av begreppet samtycke samt av skäl 32 till förordningen framgår vidare att ett samtycke ska vara ett frivilligt, specifikt, informerat och otvetydigt medgivande från den registrerades sida. Detta innebär att det ställs höga krav på tjänstetillhandahållarna att utforma informationen om vad ett samtycke innebär, särskilt i förhållande till barn, om samtycket ska ses som giltigt i förordningens mening.

Sammantaget bör den lagstiftning och branschpraxis som redan finns på marknadsföringsområdet, tillsammans med dataskyddsförordningens allmänna bestämmelser, utgöra relativt effektiva skyddsmekanismer för att förhindra omfattande insamling och annan behandling av barns personuppgifter i marknadsföringssyfte. Förordningen tillhandahåller också vissa skyddsmekanismer som balanserar riskerna med att barn lämnar samtycke till omfattande behandling utan att förstå vad det innebär, bland annat genom rätten till radering enligt artikel 17.1 f.

Sammanfattande bedömning

Det förhållandet att en åldersgräns införs innebär normalt inte att barn och unga med en ålder under gränsen kommer att utestängas från möjligheten att använda informationssamhällets tjänster. Åldersgränsen innebär dock att en förälder kommer att behöva antingen samtycka till att personuppgifter som avser barnet behandlas eller godkänna det av barnet lämnade samtycket. Eftersom ett barn som regel inte kan använda sociala medier och liknande tjänster om inte samtycke till behandling av personuppgifter ges, blir detta krav i praktiken en inskränkning i barnets rätt att fritt söka information och uttrycka sig i olika sammanhang. Det innebär också en begränsning av barnets självbestämmanderätt.

Barn i Sverige har i dag en hög medievana. Tillgången till information via söktjänster och deltagandet i olika onlineaktiviteter har

stor samhällelig och social betydelse för barn och unga. Det är ett sätt att skapa och behålla kontakt med kamrater, delta i politiska och andra diskussionsforum, söka information till skolarbeten, spela spel, se på film och lyssna på musik. En hög åldersgräns för när ett barn själv kan ge giltigt samtycke till personuppgiftsbehandling kan leda till att barn i mitten av sin tonårstid utestängs från möjligheten till social och kulturell samvaro inom ramen för det som avses med informationssamhällets tjänster, om dess vårdnadshavare inte samtycker till den personuppgiftsbehandling som krävs för att barnet ska kunna använda tjänsten. Denna oönskade effekt måste vägas emot de integritetsvinster som en hög åldersgräns skulle kunna ge.

Det har varit svårt att, inom den korta tid vi haft till vårt förfo- gande för uppdraget, klarlägga alla de omständigheter som bör påverka valet av åldersgräns. Rättsområdet är dessutom utforskat i Sverige eftersom någon liknande reglering, som skulle kunna tjäna som förebild, inte finns. Det saknas därför erfarenhet som skulle kunna ge indikationer på vilka konsekvenser de olika åldersgränserna skulle kunna ge.

En åldersgräns om 15 år är vanlig i svensk rätt när det gäller barns rätt till självbestämmande. Av harmoniseringsskäl framstår det dock inte ändamålsenligt att endast avvika från förordningens reglering med ett år och införa en åldersgräns som det kan befaras endast kommer att gälla i Sverige.

Med utgångspunkt i det som hittills har framkommit anser vi dessutom att övervägande skäl talar för att det i nuläget inte bör gälla en hög åldersgräns. Vi har då beaktat det skydd för barns personuppgifter som ges genom dataskyddsförordningens övriga bestämmelser och annan lagstiftning, t.ex. på marknadsföringsområdet. Vi har också vägt in att det i nuläget är oklart hur äktheten av föräldrarnas samtycke ska kunna verifieras vilket medför att effektiviteten kan ifrågasättas. Det skulle kunna leda till att integritetsskyddet uteblir, i fall då personuppgifterna borde skyddas men barnet utger sig för att vara föräldern som samtycker. En förslagenhet av barnet i det avseendet kan antas öka med stigande ålder. Detta ska vägas mot att en hög åldersgräns för när föräldrarna måste samtycka kan komma att hindra barn från att använda tjänsterna om barnet lyder föräldrarna trots att det uteblivna samtycket inte är motiverat av integritetsskäl. Vi känner därför tveksamhet i fråga om en hög åldersgräns leder till ett så ökat integritetsskydd att det motiverar den begräns-

ning av barns rätt till självbestämmande och yttrande- och informationsfrihet som en sådan åldersgräns skulle föranleda. Därtill kommer att det i dag inte finns någon åldersgräns alls i nu aktuellt avseende, vilket talar för att lagstiftning på området bör införas med försiktighet och inte omfatta mer än vad som kan anses absolut motiverat.

Vi anser därför att åldersgränsen för när barn ska kunna samtycka till personuppgiftsbehandling vid erbjudande av informationssamhällets tjänster bör vara så låg som förordningen medger. Vi föreslår således att åldersgränsen i Sverige i nuläget sätts till 13 år.

Om det under den fortsatta beredningen av detta betänkande, eller efter det att dataskyddsförordningen har börjat gälla, skulle visa sig att flertalet av de övriga medlemsstaterna har valt en 16-årsgräns eller en 15-årsgräns, kan det enligt vår mening finnas skäl att överväga frågan på nytt. Detsamma gäller om det skulle visa sig att det skydd som förordningens övriga bestämmelser, i kombination med övrig lagstiftning rörande bland annat marknadsföring, inte i tillräckligt hög grad skyddar barn från det integritetsintrång som kan uppstå på grund av en omfattande personuppgiftsbehandling i samband med erbjudandet av informationssamhällets tjänster direkt till barn.

10 Känsliga personuppgifter

10.1 Vårt uppdrag

Enligt kommittédirektiven ska vi överväga vilka kompletterande bestämmelser om undantag från förbudet att behandla känsliga personuppgifter i artikel 9.1 som bör finnas i den generella regleringen. För att vissa av undantagen som föreskrivs i artikel 9.2 i förordningen ska vara tillämpliga krävs enligt direktiven att grunden för sådana behandlingar kommer till uttryck i unionsrätten eller nationell rätt.

Utgångspunkten bör enligt direktiven vara att det även i fortsättningen kommer att behövas vissa bestämmelser om undantag från förbudet att behandla känsliga personuppgifter av det slag som i dag finns i personuppgiftslagen och personuppgiftsförordningen. Det ingår därför i uppdraget att analysera hur sådana bestämmelser kan utformas i den kompletterande regleringen.

10.2 Dataskyddsförordningen

I dataskyddsförordningens artikel 9.1 stadgas ett förbud mot att behandla särskilda kategorier av personuppgifter. Det gäller uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening samt genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa och uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Ett liknande förbud finns i artikel 6 i dataskyddskonventionen och i artikel 8.1 i dataskyddsdirektivet. Något färre kategorier omfattas där av förbudet; genetiska och biometriska uppgifter liksom uppgifter om sexuell läggning är nya kategorier som lagts till i dataskyddsförordningen.

I såväl direktivets som förordningens artikeltext omnämns de uppgifter som omfattas av förbudet som särskilda kategorier av personuppgifter. I förordningens skäl 10 och 51 omnämns de i stället som känsliga respektive särskilt känsliga uppgifter. I personuppgiftslagen har särskilda kategorier av personuppgifter kallats känsliga personuppgifter, utan att detta närmare har kommenterats i motiven. Det begreppet är enligt vår mening tydligare än särskilda kategorier av uppgifter, och får numera anses inarbetat även på EU-nivå.¹ Vi kommer därför fortsättningsvis att använda begreppet känsliga personuppgifter.

Förordningens förbud kompletteras liksom i direktivet av en rad undantag som möjliggör behandling av känsliga personuppgifter i vissa fall. Förbudet i sig är direkt tillämpligt genom förordningen och kräver alltså inga åtgärder av medlemsstaterna. Vissa av undantagen innehåller dock hänvisningar till nationell rätt som kan innebära att lagstiftningsåtgärder måste vidtas på nationell nivå för att undantagen ska vara tillämpliga.

10.3 Vad betyder kravet på stöd i nationell rätt?

Utredningens bedömning: Kravet på stöd i nationell rätt innebär att vissa av undantagen i sig bör föreskrivas i nationell rätt, antingen i generell eller i sektorsspecifik reglering.

Artikel 9 i förordningen lyder i sin helhet som följer. Hänvisningar till reglering på medlemsstatsnivå har kursiverats.

1. Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning ska vara förbjuden.

2. Punkt 1 ska inte tillämpas om något av följande gäller:

a) Den registrerade har uttryckligen lämnat sitt samtycke till behandlingen av dessa personuppgifter för ett eller flera specifika ändamål,

¹ Se bland annat artikel 29-gruppens Advice paper on special categories of data ("sensitive data").

utom då unionsrätten eller medlemsstaternas nationella rätt föreskriver att förbudet i punkt 1 inte kan upphävas av den registrerade.

b) Behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och på områdena social trygghet och socialt skydd, i den omfattning detta är tillåtet enligt unionsrätten eller medlemsstaternas nationella rätt eller ett kollektivavtal som antagits med stöd av medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder som säkerställer den registrerades grundläggande rättigheter och intressen fastställs.

c) Behandlingen är nödvändig för att skydda den registrerades eller någon annan fysisk persons grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.

d) Behandlingen utförs inom ramen för berättigad verksamhet med lämpliga skyddsåtgärder hos en stiftelse, en förening eller ett annat icke vinstdrivande organ, som har ett politiskt, filosofiskt, religiöst eller fackligt syfte, förutsatt att behandlingen enbart rör sådana organs medlemmar eller tidigare medlemmar eller personer som på grund av organets ändamål har regelbunden kontakt med detta och personuppgifterna inte lämnas ut utanför det organet utan den registrerades samtycke.

e) Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.

f) Behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk eller som en del av domstolarnas dömande verksamhet.

g) Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

h) Behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård, behandling, social omsorg eller förvaltning av hälso- och sjukvårdstjänster och social omsorg och av deras system, på grundval av unionsrätten eller medlemsstaternas nationella rätt eller enligt avtal med yrkesverksamma på hälsoområdet och under förutsättning att de villkor och skyddsåtgärder som avses i punkt 3 är uppfyllda.

i) Behandlingen är nödvändig av skäl av allmänt intresse på folkhälsoområdet, såsom behovet av att säkerställa ett skydd mot allvarliga gränsöverskridande hot mot hälsan eller säkerställa höga kvalitets- och säkerhetsnormer för vård och läkemedel eller medicintekniska produkter, på grundval av unionsrätten eller medlemsstaternas nationella rätt, där lämpliga och specifika åtgärder för att skydda den registrerades rättigheter och friheter fastställs, särskilt tystnadsplikt.

j) Behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, *på grundval av unionsrätten eller medlemsstaternas nationella rätt*, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

3. Personuppgifter som avses i punkt 1 får behandlas för de ändamål som avses i punkt 2 h, när uppgifterna behandlas av eller under ansvar av en yrkesutövare som omfattas av *tystnadsplikten enligt unionsrätten eller medlemsstaternas nationella rätt* eller bestämmelser som fastställs av nationella behöriga organ eller av en annan person som också omfattas av *tystnadsplikten enligt unionsrätten eller medlemsstaternas nationella rätt* eller bestämmelser som fastställs av nationella behöriga organ.

4. Medlemsstaterna *får behålla eller införa ytterligare villkor*, även begränsningar, för behandlingen av genetiska eller biometriska uppgifter eller uppgifter om hälsa.

Det är alltså i artikel 9.2 a (samtycke), b (arbetsrätt m.m.), g (viktigt allmänt intresse), h (hälso- och sjukvård), i (folkhälsa) och j (arkiv och statistik) samt i artikel 9.3 och 9.4 som hänvisningar finns till medlemsstaternas nationella rätt. Bestämmelserna innehåller också krav på någon form av skyddsåtgärder. Formuleringarna skiljer sig något åt. I vissa fall krävs lämpliga skyddsåtgärder (artikel 9.2 b), i andra lämpliga och särskilda åtgärder (artikel 9.2 g och 9.2 j) eller lämpliga och specifika åtgärder (artikel 9.2 i).

Det är inte helt klart vilken innebörd hänvisningarna till och kraven på nationell rätt har eller vilken betydelse det har att de utformats på olika sätt. Det finns några uttalanden i förordningens skäl som rör känsliga personuppgifter och kraven på stöd i nationell rätt. I skäl 10 sägs att förordningen är avsedd att ge medlemsstaterna handlingsutrymme att specificera bestämmelser för behandlingen av känsliga uppgifter samt att förordningen inte utesluter att det fastställs närmare omständigheter och mer exakta villkor för laglig behandling av personuppgifter. Skäl 51 och 52 rör också känsliga personuppgifter. Nämnade skäl är inte helt entydiga, men i skäl 52 nämns att vissa undantag från förbudet att behandla känsliga personuppgifter bör tillåtas *om de föreskrivs* (when provided for) i unionsrätten eller i medlemsstaternas nationella rätt och underkastas lämpliga skyddsåtgärder.

I rådets ståndpunkt inför antagandet av förordningen (dok 5419/1/16 REV 1 ADD 1) sägs angående undantag från förbudet att behandla känsliga personuppgifter att sådana undantag tillåts om behandlingen i fråga grundar sig på unionsrätten eller medlemsstaternas nationella rätt.

Inte heller ovan nämnda formuleringar ger något klart och entydigt svar på frågan vad hänvisningarna till nationell rätt innebär. Texten i skäl 52 skulle kunna tala för att undantagen i sig måste tas in i nationell rätt för att bli tillämpliga, medan en mer enhetlig tolkning av förordningens artikel 6 och artikel 9 möjligen talar för att det snarare är verksamheten i sig som ska vara reglerad (jämför avsnitt 8.3.1).

Oavsett hur hänvisningarna till nationell rätt i artikel 9 ska tolkas menar vi, mot bakgrund av uttalandena i skäl 10, att en reglering och specificering av undantagen på nationell nivå inte är oförenlig med förordningen. Här beaktar vi också skrivningarna i skäl 8, där det tydliggörs att förordningen medger att medlemsstaterna i viss utsträckning införlivar delar av förordningen i nationell rätt. I vissa fall, såsom när det gäller undantaget för viktiga allmänna intressen, talar också förordningens krav på särskilda skyddsåtgärder för att såväl undantaget som skyddsåtgärderna bör regleras och preciseras i nationell rätt för att få någon substans.

Det är inte självklart att de undantag som i så fall föreskrivs måste finnas i dataskyddslagen. Av formuleringarna i skäl 10 framgår att de närmare villkoren för sådan behandling får regleras på mer detaljerad nivå, vilket öppnar för en sektorsspecifik reglering. Det faktum att förordningens formuleringar angående stödet i nationell rätt och de skyddsåtgärder medlemsstaterna förväntas uppställa varierar i de olika undantagen, liksom undantagens skilda karaktär, gör att det för vart och ett av undantagen bör göras en bedömning av behovet och lämpligheten av en generell reglering i dataskyddslagen. För att tydliggöra förhållandet mellan de undantag från förbudet att behandla känsliga personuppgifter som bedöms lämpliga att föra in i dataskyddslagen och de direkt tillämpliga undantag som gäller enligt förordningens artikel 9.2 bör en upplysningsbestämmelse tas in i dataskyddslagen.

Överväganden och förslag när det gäller behandling av känsliga personuppgifter för arkiv- och statistikändamål finns i avsnitt 14.

10.4 Den registrerades samtycke

10.4.1 Gällande rätt

I dataskyddsdirektivets artikel 8.2 a stadgas en möjlighet för medlemsstaterna att lagstifta bort verkan av den registrerades samtycke när det gäller känsliga personuppgifter. Vid införandet av personuppgiftslagen ansåg Datalagskommittén att den enskilde, vars integritet ska skyddas, själv bör få avgöra om en behandling av hans eller hennes uppgifter får ske.² Regeringen ansåg inte heller att det fanns något integritetsskyddsintresse som gjorde det befogat att förbjuda en behandling som den registrerade och den personuppgiftsansvarige var överens om. Det infördes därför varken någon sådan bestämmelse i lag eller någon möjlighet för regeringen eller Datainspektionen att föreskriva något förbud mot behandling trots den registrerades samtycke.³

10.4.2 Överväganden

Utredningens bedömning: Den registrerades uttryckliga samtycke bör även fortsättningsvis medföra att känsliga personuppgifter får behandlas.

I förordningens artikel 9.2 a finns liksom i dataskyddsdirektivet en möjlighet för medlemsstaterna att föreskriva att den registrerade inte kan samtycka till behandling av känsliga personuppgifter. Något som talar för att det nu bör införas ett förbud mot behandling trots den registrerades samtycke har inte framkommit. Vi instämmer därför i de skäl som anförts i motiven till personuppgiftslagen. Att behandling av känsliga personuppgifter får ske då den registrerade har lämnat sitt samtycke framgår direkt av artikel 9.2 a och behöver inte föreskrivas. Det innebär att vi bedömer att någon nationell reglering inte bör införas på grund av artikel 9.2 a.

² SOU 1997:39 s. 373.

³ Prop. 1997/98:44 s. 69.

10.5 Arbetsrätt, social trygghet och socialt skydd

10.5.1 Gällande rätt

Dataskyddsdirektivet föreskriver ett undantag från förbudet mot behandling av känsliga personuppgifter på arbetsrättens område i artikel 8.2 b. Artikeln har genomförts i svensk rätt genom punkt a i 16 § första stycket PUL. Där framgår det att känsliga personuppgifter får behandlas om behandlingen är nödvändig för att den registeransvarige ska kunna fullgöra sina skyldigheter eller utöva sina rättigheter inom arbetsrätten.

Datalagskommittén ansåg att i stort sett alla skyldigheter och rättigheter för arbetsgivare beträffande de anställda och deras organisationer borde kunna innefattas i uttrycket inom arbetsrätten, exempelvis behandling i samband med sjuklön och rehabilitering av arbetstagare. Även skyldigheter och rättigheter för fackliga organisationer i förhållande till arbetsgivare och deras organisationer borde enligt kommittén innefattas. De skyldigheter och rättigheter som avsågs var enligt kommittén sådana som åligger den personuppgiftsansvarige enligt lag, myndighetsbeslut, kollektivavtal eller andra avtal.⁴

Enligt artikel 8.2 b i direktivet måste den nationella lagstiftningen också föreskriva lämpliga skyddsåtgärder. Vid genomförandet av direktivet ansågs att en tillräcklig skyddsåtgärd var att föreskriva att de behandlade uppgifterna fick lämnas ut till tredje man bara om det finns en uttrycklig skyldighet för den persondataansvarige att göra det inom arbetsrätten eller den registrerade har samtyckt till utlämnandet.⁵ En sådan bestämmelse infördes i 16 § andra stycket PUL.

10.5.2 Överväganden och förslag

Utredningens förslag: Känsliga personuppgifter ska få behandlas om det är nödvändigt för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten. Uppgifter ska få lämnas ut till tredje part endast om det finns en skyldighet inom arbetsrätten

⁴ SOU 1997:39 s. 372 f.

⁵ SOU 1997:39 s. 375.

för den personuppgiftsansvarige att göra det, eller om den registrerade uttryckligen har samtyckt till utlämnandet.

Utredningens bedömning: Något undantag för behandling av känsliga personuppgifter på områdena social trygghet och socialt skydd bör inte införas i dataskyddslagen.

I dataskyddsförordningen har direktivets bestämmelse om undantag för att den personuppgiftsansvarige ska kunna fullgöra rättigheter och skyldigheter inom arbetsrätten utvidgats, till att avse även den registrerades rättigheter och skyldigheter samt områdena social trygghet och socialt skydd (artikel 9.2 b). Förordningen förtydligar också att behandlingen kan vara tillåten enligt kollektivavtal. Förordningen förutsätter liksom direktivet att lämpliga skyddsåtgärder fastställs, med tillägget att skyddsåtgärderna ska säkerställa den registrerades grundläggande rättigheter och intressen. Undantaget gäller i den omfattning behandlingen är tillåten enligt nationell rätt och under förutsättning att lämpliga skyddsåtgärder som säkerställer den registrerades grundläggande rättigheter och intressen fastställs.

Arbetsrätt

Undantaget avseende arbetsrätt är tillämpligt generellt i alla sektorer av samhället. Det finns i dag inte någon sektorsspecifik reglering som kan utgöra grund för sådan behandling som avses i artikeln, och inte heller någon generell tillämplig reglering om tystnadsplikt eller andra bestämmelser som tillgodoser förordningens krav på skyddsåtgärder.

För att möjliggöra sådan nödvändig behandling som avses i artikeln och samtidigt tillgodose kravet på skyddsåtgärder menar vi att det finns behov av en generell reglering även fortsättningsvis. En begränsning av möjligheten att lämna ut uppgifter till utomstående framstår som en i sammanhanget effektiv och lämplig skyddsåtgärd. Med de justeringar som föranleds av förordningstexten framstår därför en liknande bestämmelse som den som finns i punkten a i 16 § första stycket PUL samt andra stycket i samma paragraf som lämplig.

Termen arbetsrätt i detta sammanhang har en EU-rättslig innebörd, men bör enligt vår mening i avvaktan på närmare vägledning ges den tolkning som den har vid tillämpningen av personuppgiftslagen.

Den skyldighet att lämna ut personuppgifter som avses i 16 § andra stycket PUL måste enligt motiven framgå av lagstiftning, myndighetsbeslut eller av ett muntligt eller skriftligt avtal.⁶ Detsamma bör gälla även fortsättningsvis. Att undantaget i artikel 9.2 b gäller även behandling som sker enligt kollektivavtal framgår direkt av artikeltexten. Bestämmelsen i artikeln innebär också att lämpliga skyddsåtgärder måste framgå av avtalet.

Begreppet tredje part har i förordningen ersatt begreppet tredje man och bör alltså användas i den reglering vi föreslår. Tredje part definieras i förordningens artikel 4.10 som en fysisk eller juridisk person, offentlig myndighet, institution eller organ som inte är den registrerade, den personuppgiftsansvarige, personuppgiftsbiträdet eller de personer som under den personuppgiftsansvariges eller personuppgiftsbitrådets direkta ansvar är behöriga att behandla personuppgifterna. Detta innebär exempelvis att en arbetsgivares utlämnande till en facklig organisation omfattas av den föreslagna regleringen om utlämnande.

Social trygghet och socialt skydd

Det är inte helt klart vad som avses med tilläggen social trygghet och socialt skydd i artikel 9.2 b (på engelska *social security and social protection law*, och på franska *le droit de la sécurité sociale et de la protection sociale*). Skäl 52 i förordningen indikerar att undantaget är avsett att omfatta ”behandling av personuppgifter inom ramen för arbetsrätt och sociallagstiftning, däribland pensioner”.

Begreppet sociallagstiftning brukar i svensk rätt avse lagstiftning som socialtjänstlagen, lagen med särskilda bestämmelser om vård av unga, lagen (1988:870) om vård av missbrukare och lagen om stöd och service till vissa funktionshindrade. Begreppet social trygghet i artikeltexten och omnämmandet av pensioner i skäl 52 skulle också kunna tala för att behandling av personuppgifter på socialförsäkringsområdet, dvs. avseende sjukförsäkringar, pensioner och föräldraförsäkring, omfattas av undantaget. Personuppgiftsbehandling på dessa områden är i dag reglerad i sektorsspecifik lagstiftning.⁷

⁶ Prop. 1997/98:44 s. 124.

⁷ Lagen (2001:454) om behandling av personuppgifter inom socialtjänsten och 114 kap. socialförsäkringsbalken.

Sociallagstiftning och den lagstiftning som återfinns på socialförsäkringsområdet tycks sakligt sett ligga långt ifrån arbetsrätten, vilket talar emot att det skulle vara behandling av uppgifter i sådan verksamhet som avses i detta sammanhang. Behandling av känsliga personuppgifter i sådan verksamhet bör kunna ske med stöd av den reglering vi föreslår för myndigheters behandling som är nödvändig med hänsyn till ett viktigt allmänt intresse, i den mån den inte är sektorsspecifikt reglerad. Det kan exempelvis noteras att i direktivets skäl 34 tas sjukförsäkringar upp som ett sådant viktigt allmänt intresse som avses i direktivets motsvarande bestämmelse. Någon liknande skrivning finns dock inte i förordningen.

Vi bedömer det mot bakgrund av ovanstående som osannolikt att artikeln skulle vara avsedd att täcka personuppgiftsbehandling inom de områden som motsvarar den svenska sociallagstiftningen eller lagstiftningen på socialförsäkringsområdet.

Med tanke på det sammanhang där begreppen social trygghet och socialt skydd förekommer bedömer vi i stället att avsikten sannolikt är att reglera behandling som är nödvändig för att arbetsgivare, fackförbund eller arbetsgivarorganisationer ska kunna erbjuda eller förmedla pensioner och försäkringar med anknytning till den registrerades anställning eller yrkesliv, såsom tjänstepensioner och olika typer av gruppförsäkringar. Den behandling av känsliga personuppgifter som är nödvändig hos en arbetsgivare för sådana syften torde i dag i många fall kunna ske med stöd av undantaget om arbetsrätt i punkten a i 16 § första stycket PUL.

Vår bedömning är att den behandling som tillåts i artikel 9.2 g inom områdena social trygghet och socialt skydd i många fall kommer att kunna ske med stöd av undantaget som rör arbetsrätt eller undantaget som rör viktiga allmänna intressen. Om inget av dessa undantag är tillämpliga torde behandlingen i vissa situationer i stället kunna ske med stöd av samtycke. Vi ser inget behov av att i data-skyddslagen, på generell nivå, införa denna del av det aktuella undantaget. Av förordningens artikel 9.2 b framgår som nämnts ovan att behandling enligt undantaget bara gäller *i den omfattning detta är tillåtet* enligt unionsrätten eller medlemsstaternas nationella rätt eller enligt ett kollektivavtal. Vår bedömning är därför att förordningen inte hindrar att undantaget endast införs delvis i nationell rätt. Om begreppen social trygghet och socialt skydd skulle visa sig få en annan

EU-rättslig innebörd än vad som förutsatts här, får vår nationella reglering ses över för att säkerställa att förordningens krav efterlevs.

10.6 Viktigt allmänt intresse

10.6.1 Gällande rätt

Av artikel 8.4 i dataskyddsdirektivet framgår att undantag från förbudet mot behandling av känsliga personuppgifter får göras av hänsyn till ett viktigt allmänt intresse, förutsatt att sådana undantag förses med lämpliga skyddsåtgärder. Det finns ingen legaldefinition eller exemplifiering av vad som avses med skyddsåtgärder i direktivet. Med stöd av artikeln har olika typer av undantag införts i medlemsstaterna, bland annat för behandling av känsliga personuppgifter i myndigheters verksamhet, på bankområdet och för att främja jämställdhet och social trygghet.⁸

I personuppgiftslagen har undantaget som rör viktiga allmänna intressen genomförts dels genom regleringen av behandling för forsknings- och statistikändamål i 19 § PUL, dels genom ett bemyndigande i 20 § PUL för regeringen eller den myndighet som regeringen bestämmer att föreskriva ytterligare undantag om det behövs med hänsyn till ett viktigt allmänt intresse. När det gäller bemyndigandet i 20 § PUL resoneras inte närmare i motiven kring vilka skyddsåtgärder som krävs när regeringen eller Datainspektionen meddelar föreskrifter. Det konstateras bara att regeringen och inspektionen måste hålla sig inom den ram som direktivet ställer upp.⁹

Bemyndigandet i 20 § PUL har bland annat utnyttjats genom att det har införts en bestämmelse i 8 § PUF om att känsliga personuppgifter får behandlas av en myndighet i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det. Bestämmelsen gäller utöver den behandling som är tillåten enligt den så kallade missbruksregeln i 5 a § PUL och undantagen i 15–19 §§ PUL. Bestämmelsen i 8 § PUF har inte ansetts omfatta så kallad faktisk verksamhet som en myndighet bedriver.¹⁰ Med faktisk verksamhet kan avses t.ex. viss vård och behandling, rådgivning,

⁸ Artikel 29-gruppens Advice paper on special categories of data ("sensitive data"), s. 7.

⁹ SOU 1997:39 s. 329.

¹⁰ SOU 2015:39 s. 304.

uppföljning eller samverkan utan ärendanknytning. Behandling av känsliga personuppgifter som förekommer i sådan verksamhet hämtar sannolikt sitt stöd i missbruksregeln i 5 a § PUL.

Det finns också andra exempel än 8 § PUF på när bemyndigandet har utnyttjats för att på förordningsnivå föreskriva att myndigheter får behandla känsliga personuppgifter, t.ex. i 9 § förordningen (2002:710) med instruktion för Folke Bernadotteakademin, samt 6 och 7 §§ förordningen (2006:275) om behandling av personuppgifter i utrikesförvaltningens konsulära verksamhet. Det har också förekommit att regeringen beslutat om bestämmelser om privata aktörers behandling av känsliga personuppgifter på grund av viktiga allmänna intressen med stöd av 20 § PUL, exempelvis 3 kap. 13 § läkemedelsförordningen (2015:458), där det stadgas att innehavare av ett godkännande eller en registrering för försäljning av läkemedel får utföra behandling av personuppgifter som rör hälsa om det är nödvändigt för att de ska kunna fullgöra vissa skyldigheter.

Även i övrigt har artikel 8.4 i direktivet utgjort grund för bestämmelser i en mängd sektorsspecifika författningar, vilka medger behandling av känsliga personuppgifter på olika områden. Bland annat har tillsynsverksamheten hos Inspektionen för socialförsäkringen ansetts utgöra ett viktigt allmänt intresse, liksom att socialtjänsten kan utföra sina arbetsuppgifter på ett tillfredsställande sätt.¹¹ I svensk rätt har alltså begreppet viktigt allmänt intresse ansetts omfatta även sådan verksamhet som innefattar myndighetsutövning.

10.6.2 Överväganden och förslag

Utredningens förslag: Särskilda undantag från förbudet mot behandling av personuppgifter bör införas för myndigheter.

Myndigheter ska få behandla känsliga personuppgifter i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det. Vidare ska myndigheter och andra organ som omfattas av offentlighetsprincipen få behandla känsliga personuppgifter om dessa har lämnats till myndigheten eller organet och behandlingen krävs enligt lag. Dessutom ska myndigheter i enstaka fall få behandla känsliga personuppgifter om det är abso-

¹¹ Prop. 2000/01:80 s.144 och SOU 2014:67 s. 112.

lut nödvändigt för ändamålet med behandlingen och behandlingen inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

Ett förbud för myndigheter att använda sökbegrepp som avslöjar känsliga personuppgifter ska också införas, i fall då behandlingen sker enbart med stöd av de nämnda undantagen.

Regeringen ska få meddela föreskrifter om ytterligare undantag från förbudet mot behandling av känsliga personuppgifter om det behövs med hänsyn till ett viktigt allmänt intresse.

Begreppet viktigt allmänt intresse

Av artikel 9.2 g framgår att känsliga personuppgifter får behandlas om behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av nationell rätt. Samtidigt förekommer begreppet allmänt intresse i artikel 6.1 e. Båda begreppen är unionsrättsliga, och finns även i dataskyddsdirektivet (artiklarna 7 e och 8.4). Olika varianter på begreppen återfinns, förutom i de nämnda artiklarna, i artikel 23.1 e och artikel 49 d i dataskyddsförordningen. Vad som är ett allmänt intresse respektive ett viktigt allmänt intresse är dock inte definierat i vare sig dataskyddsdirektivet eller dataskyddsförordningen, och begreppens innebörd har inte heller utvecklats av EU-domstolen.

I avsnitt 8.3.4 bedömer vi att det med hänsyn till svensk förvaltningstradition är rimligt att anta att alla uppgifter som utförs av statliga myndigheter i syfte att uppfylla ett uttryckligt uppdrag av riksdag eller regering är av allmänt intresse, och att de obligatoriska uppgifter som utförs av kommuner och landsting till följd av deras åligganden enligt lag eller förordning, är av allmänt intresse i dataskyddsförordningens mening.

Det kan noteras att i kommissionens ursprungliga förordningsförslag föreslogs att begreppet allmänt intresse skulle användas i artikel 9, i stället för viktigt allmänt intresse. Ordet ”viktigt” fördes dock tillbaka under förhandlingarna i rådet. Detta talar för att begreppet i artikel 9 är något snävare än begreppet i artikel 6.

Det är svårt att på ett generellt plan definiera vad som skiljer en uppgift av allmänt intresse enligt artikel 6.1 e från sådana viktiga allmänna intressen som kan motivera behandling av känsliga person-

uppgifter enligt artikel 9.2 g. Utgångspunkten för våra fortsatta överväganden när det gäller myndigheters behandling är att det måste anses utgöra ett viktigt allmänt intresse att svenska myndigheter kan bedriva den verksamhet som tydligt faller inom ramen för deras uppdrag på ett korrekt, rättssäkert och effektivt sätt. Vilken behandling av känsliga personuppgifter som är nödvändig av hänsyn till detta intresse får bedömas när myndigheternas behandling av personuppgifter blir föremål för författningsreglering nationellt. Vi avser att återkomma till den frågan nedan, när det gäller hur ett generellt tillämpligt undantag för myndigheter bör utformas i dataskyddslagen. Det kan dock finnas anledning att erinra om att även om viss behandling av känsliga personuppgifter är tillåten enligt dataskyddslagen eller sektorsspecifik reglering måste den i det enskilda fallet också leva upp till dataskyddsförordningens krav i övrigt, exempelvis principerna för behandling i artikel 5.

Förordningens krav på skyddsåtgärder förklaras inte närmare i förordningstext eller skäl. Artikel 29-gruppen har inför dataskyddsreformen efterfrågat en definition av begreppet och exemplifieringar av sådana åtgärder, men någon definition har inte införts i förordningen.

En särskild myndighetsreglering

Myndigheter har ofta berättigade skäl att behandla känsliga personuppgifter, och i många fall sker behandlingen i den registrerades eget intresse. Det finns därför ett behov av en tydlig reglering som tillåter viss behandling av känsliga personuppgifter hos myndigheterna. I många fall finns sådana regler i sektorsspecifika författningar. Det behov av att behandla känsliga personuppgifter som därutöver finns hos myndigheter är i dag tillgodosett genom att viss behandling är tillåten enligt 8 § PUF och genom missbruksregeln i 5 a § PUL. Vi bedömer att det även fortsättningsvis finns behov av generellt tillämpliga undantag, som ska gälla i de fall där sektorsspecifik reglering saknas.

Förordningens krav på att behandlingen ska vara nödvändig för ett viktigt allmänt intresse utgör en grundläggande begränsning av myndigheternas möjligheter till behandling. Det är inte helt klart i vilken mån kravet på nödvändighet innebär något ytterligare för myndig-

heternas del än det nödvändighetskrav som återfinns redan i villkoren för laglig behandling i artikel 6.1 c och e i dataskyddsförordningen. Sannolikt innebär kravet på nödvändighet i artikel 9 enbart en erinran om att behovet av att behandla just de känsliga personuppgifterna ska prövas mot det något striktare kravet på ”viktigt allmänt intresse”. I detta sammanhang förtjänar det att påpekas att unionsrättsligt har nödvändighetsrequisitet inte ansetts utgöra ett krav på att det ska vara omöjligt att fullgöra förpliktelsen eller utföra uppgiften utan att behandlingsåtgärden vidtas.¹²

Informationshanteringsutredningen föreslog en bestämmelse om behandling av känsliga personuppgifter hos myndigheter av följande lydelse.¹³

Utöver vad som följer av 15, 16, 18 och 19 §§ personuppgiftslagen (1998:204) får känsliga personuppgifter behandlas om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggning av det eller om uppgifterna behandlas endast i löpande text.

Utredningen menade bland annat att förslaget skulle tillgodose behovet av en reglering som möjliggör behandling av känsliga personuppgifter inom ramen för ett ärendehanteringssystem, oavsett om de förekommer i löpande text eller inte. Förslaget innebar också att missbruksregeln inte skulle tillämpas på myndigheters behandling av känsliga personuppgifter.

Förslaget kritiserades av flera remissinstanser, bland andra Datainspektionen och Advokatsamfundet. Datainspektionen ansåg att begränsningen till vad som är nödvändigt för handläggningen av ett ärende inte innebar en tillräckligt restriktiv utformning av bestämmelsen eftersom det potentiella integritetsintrånget skulle bero på hur myndigheterna väljer att avgränsa sina ärenden. Inspektionen kritiserade också att förslaget inte innehöll någon begränsning till uppgifter i löpande text. Advokatsamfundet menade att den nuvarande regleringen i 8 § PUF borde ha tagits in oförändrad i förslaget.

Mot bakgrund av den remisskritik som uttalats mot Informationshanteringsutredningens förslag är vår utgångspunkt att någon större utvidgning av myndigheternas möjligheter att behandla känsliga personuppgifter inte bör införas genom den dataskyddslag vi föreslår. En

¹² Dom Huber mot Tyskland, C-524/06, EU:C:2008:724.

¹³ SOU 2015:39 s. 39, 10 § i förslaget till myndighetsdatalag.

tydligt utvidgad möjlighet att behandla känsliga personuppgifter hos myndigheter måste föregås av en mer ingående analys av konsekvenserna ur ett integritetsperspektiv, som vi inte bedömer är möjlig att genomföra inom ramen för vårt uppdrag.

Behandling i löpande text

I dag har myndigheter enligt 8 § PUF möjlighet att behandla känsliga personuppgifter i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det. Detta möjliggör till exempel att känsliga personuppgifter får finnas i skälen till ett beslut, när det krävs för att beslutet ska uppfylla kraven enligt förvaltningslagen (1986:223). Med de avgränsningar bestämmelsen har till myndigheters ärendehandläggning bedömer vi att sådan behandling får anses nödvändig av hänsyn till ett viktigt allmänt intresse och att den bör möjliggöras genom en bestämmelse i dataskyddslagen.¹⁴ Begränsningen till löpande text bör dock inte utesluta att handlingar med ostrukturerade känsliga personuppgifter lagras elektroniskt i ärendehanteringssystem eller liknande. Skyddet för uppgifterna bör i stället upprätthållas genom ett sökförbud, se nedan.

Behandling som krävs på grund av annan lag

Att myndigheterna ska kunna sköta sitt uppdrag på ett korrekt, rättssäkert och effektivt sätt måste som vi konstaterat tidigare anses vara ett viktigt allmänt intresse. Detta förutsätter att den grundlagsstadgade handlingsoffentligheten och andra lagstadgade skyldigheter upprätthålls. Viss behandling av känsliga personuppgifter är oundviklig i myndigheternas verksamhet som en direkt följd av exempelvis tryckfrihetsförordningens, offentlighets- och sekretesslagens och förvaltningslagens krav när det gäller inkomna handlingar, såsom krav på diarieföring och skyldighet att ta emot e-post. Myndigheternas skyldigheter enligt nämnda lagar är inte begränsade till behandling som sker inom ramen för ärendehandläggning eller i löpande text. Samma skyldigheter gäller i viss utsträckning för vissa andra organ än myndigheter, som en följd av att dessa organ jämställs med myndigheter

¹⁴ En liknande bedömning gjordes i SOU 2004:6 s. 115 f.

enligt offentlighets- och sekretesslagen. Sådan behandling bör uttryckligen tillåtas i dataskyddslagen så att det inte råder någon tveksamhet kring lagligheten av behandlingen.

Absolut nödvändig behandling i andra fall

Behandling av känsliga personuppgifter kan vidare vara berättigad även i vissa situationer utöver behandling i löpande text med koppling till ett visst ärende, eller då behandlingen inte direkt krävs enligt annan lag. Så kan exempelvis vara fallet i faktisk verksamhet såsom i kommunikation mellan skola och föräldrar eller inom en myndighet i samband med utvärdering. Enligt nuvarande ordning ges möjlighet till sådan behandling med stöd av missbruksregeln i 5 a § PUL, vilken bland annat innebär att behandling får ske i ostrukturerat material om den inte innebär en kränkning av den registrerades personliga integritet. Denna formulering i 5 a § PUL innebär att bedömningen ska ta sin utgångspunkt i vilket sammanhang uppgifterna förekommer, för vilket syfte de behandlas och vilken spridning uppgifterna har fått.¹⁵ Formuleringen har också ansetts medföra att en intresseavvägning måste ske i det enskilda fallet.¹⁶

Vår utgångspunkt är att dataskyddslagen bör ge utrymme för behandling i motsvarande situationer efter en prövning i det enskilda fallet. Behandlingen måste dock regleras på ett sätt som beaktar förordningens krav på proportionalitet och skyddsåtgärder. För att uppnå detta i en bestämmelse som avser samtliga myndigheter är det vår bedömning att regleringen bör innehålla vissa klart begränsande rekvisit. Det bör därför framgå av författningstexten att undantaget ska gälla för behandling i enstaka fall.

Ett rekvisit som använts såväl i unionsrätten som i svensk rätt för att markera restriktivitet är begreppet absolut nödvändigt. Begreppet ska inte förväxlas med det unionsrättsliga begreppet nödvändigt, vilket som nämnts tidigare har fått en något annorlunda betydelse än det har i svenskt språkbruk (jfr avsnitt 8.2.2).

Begreppet absolut nödvändigt återfinns bland annat i artikel 10 och artikel 39.1 a i det nya dataskyddsdirektivet ("strictly necessary" i

¹⁵ Prop. 2005/06:173 s. 59.

¹⁶ Öman och Lindblom, Personuppgiftslagen (20 december 2016, Zeteo), kommentaren till 5 a § PUL.

den engelska versionen). Av skäl 72 i nya dataskyddsdirektivet framgår att man med rekvisitet absolut nödvändigt i artikel 39.1 a – som rör överföring av uppgifter till mottagare som är etablerade i tredje länder – avsett att regleringen ska tillämpas restriktivt och inte möjliggöra upprepade, omfattande, strukturella eller storskaliga överföringar. Det finns också ett flertal exempel på hur begreppet absolut nödvändigt har använts i svensk rätt i sektorsspecifika författningar som har antagits på senare tid, exempelvis i 2 kap. 8 § åklagardatalagen (2015:433) och 15 § utlänningsdatalagen, för att markera särskild restriktivitet och betona vikten av en prövning i det enskilda fallet.

Vår avsikt är att markera att behandling av känsliga personuppgifter i här aktuella fall bara ska ske efter en noggrann prövning i det enskilda fallet. Enligt vår bedömning ger rekvisitet absolut nödvändigt uttryck för den avsikten på ett rättvisande sätt.

Prövningen bör också ske med beaktande av vilket intrång behandlingen utgör i den registrerades integritet. Vi föreslår därför att en avvägning ska göras av om en i och för sig absolut nödvändig behandling av känsliga personuppgifter ändå innebär ett otillbörligt intrång i den registrerades identitet. Begreppet otillbörligt intrång används bland annat i 19 § andra stycket PUL, och förekom redan i 3 § datalagen (1973:289).

Av 3 § datalagen och motiven till den bestämmelsen framgår att det vid bedömningen av om en behandling utgjorde ett otillbörligt intrång skulle läggas vikt vid sådana aspekter som uppgifternas känslighet, den inställning de registrerade kunde antas ha till att uppgifter om dem behandlades, den spridning de skulle komma att få och risken för vidarebehandling för andra ändamål än insamlingsändamålet.¹⁷ Sådana aspekter bör vara vägledande även vid tillämpningen av den bestämmelse vi föreslår. Den närmare betydelsen av begreppet otillbörligt intrång bör dock inte slås fast, utan ges utrymme att utvecklas i rättstillämpningen. Om en domstol skulle bedöma att en absolut nödvändig behandling ändå utgör ett otillbörligt intrång och därmed inte är tillåten, bör lagstiftaren överväga om ett sektorsspecifikt undantag med mer precisa avvägningar och begränsningar behövs för att myndigheten ska kunna bedriva sin verksamhet på det aktuella området.

¹⁷ Prop. 1973:33 s. 94 f.

Sökförbud

Eftersom den reglering vi föreslår för myndigheters behandling av känsliga personuppgifter inte är avgränsad till visst område, viss verksamhet eller en viss typ av ärenden bedömer vi att ytterligare åtgärder bör införas för att leva upp till förordningens krav på lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

En vanligt förekommande skyddsåtgärd i befintliga sektorsspecifika författningar är sökbegränsningar. Vi menar att en sökning som avslöjar och sammanställer känsliga personuppgifter är en åtgärd som i sig innebär en integritetskränkning. Företeelsen ligger nära det som ursprungligen har motiverat förbudet mot behandling av känsliga personuppgifter, nämligen möjligheten att kartlägga personer på grundval av exempelvis etnicitet eller politiska åsikter. Med ett sökförbud uppnås ett relativt effektivt skydd av just de intressen som bestämmelserna om känsliga personuppgifter ska värna.

Ett sådant sökförbud innebär i svensk rätt också att offentlighetsprincipen inskränks enligt den så kallade begränsningsregeln i 2 kap. 3 § tredje stycket tryckfrihetsförordningen. En begäran att få tillgång till en sammanställning av uppgifter som är resultatet av en sådan förbjuden sökning ska alltså avslås på den grunden att sammanställningen inte anses förvarad hos myndigheten. Att sammanställningar av känsliga personuppgifter inte lämnas ut framstår som en inte obetydlig integritetsvinst för de registrerade. Det bör dock understrykas att begränsningsregeln inte hindrar att sökningar görs i färdiga elektroniska handlingar vid en begäran om tillgång till allmänna handlingar. Sökning får alltså på begäran ske i upptagningar där myndigheten eller den som lämnat in handlingen till myndigheten har gett upptagningen ett bestämt, fixerat, innehåll som går att återskapa gång på gång.

Med beaktande av vad som nämnts ovan om skyddseffekterna av ett sökförbud föreslår vi att myndigheters möjligheter att använda sökbegrepp som avslöjar känsliga personuppgifter ska begränsas. Ett alternativ vi har övervägt är att föreslå ett generellt sökförbud för myndigheter, oavsett på vilket undantag de stödjer sin behandling. Konsekvenserna av ett generellt tillämpligt sökförbud är dock svåra att överblicka, såväl vad gäller effekterna på handlingsoffentligheten som när det gäller myndigheternas praktiska verksamhet. Det är

vidare tveksamt om ett sökförbud som gäller även för behandling som sker med stöd av direkt tillämpliga undantag i artikel 9 skulle vara förenligt med förordningen.

Vi har mot denna bakgrund bedömt att sökförbudet bör begränsas till fall då behandlingen sker enbart med de generella myndighetsundantagen som grund. Det innebär exempelvis att sökförbudet inte kommer att gälla när behandling sker i myndigheters personaladministrativa verksamhet med stöd av det föreslagna undantaget på arbetsrättens område. I praktiken kan sökförbudets utformning därför komma att få effekter på hur myndigheterna organiserar sin personuppgiftsbehandling, genom att hanteringen av personaladministrativa uppgifter skiljs från behandling som huvudsakligen sker med stöd av de generella myndighetsundantagen. Detta torde dock vara fallet redan i dag, eftersom uppgifter i den personaladministrativa verksamheten omfattas av särskilda sekretessregler och som regel behandlas av en begränsad krets personer. Vår bedömning är att merparten av den behandling av känsliga personuppgifter som sker i myndigheternas verksamhet i övrigt kommer att behöva ske med stöd av de föreslagna myndighetsundantagen, när sektorsspecifik reglering inte finns.

Sökförbudet bör omfatta alla typer av tekniska åtgärder som innebär att uppgifter används för att strukturera eller systematisera information så att känsliga personuppgifter avslöjas.

Sektorsspecifik reglering och normnivå

De här föreslagna undantagen är avsedda att vara generellt tillämpliga regler som ska gälla för myndigheter i verksamhet som inte har någon sektorsspecifik reglering av sin behandling av känsliga personuppgifter. Det kan finnas anledning att för vissa sektorer närmare precisera och avgränsa möjligheterna att behandla känsliga personuppgifter mer än i de här föreslagna undantagen. Ett berättigat behov av att behandla känsliga personuppgifter i större omfattning än vad dessa undantag medger, exempelvis ett behov av att använda sökbegrepp som avslöjar känsliga personuppgifter, kommer också att finnas i vissa verksamheter. Det finns då, precis som i dag, möjlighet att införa sektorsspecifik reglering som är mer tillåtande – exempelvis genom undantag från sökförbudet – så länge dessa undantag utfor-

mas så att de är förenliga med regeringsformens och dataskyddsförordningens bestämmelser. En viktig aspekt att beakta är då givetvis förordningens krav på proportionalitet, förenlighet med det väsentliga innehållet i rätten till dataskydd och kravet på skyddsåtgärder. I detta sammanhang förtjänar det återigen att påpekas att all behandling, även sådan behandling av känsliga personuppgifter som har stöd i sektorsspecifik författning, måste leva upp till förordningens krav i det enskilda fallet, exempelvis de grundläggande kraven på behandling i artikel 5.

Den enda generella reglering av myndigheternas behandling av känsliga personuppgifter som finns i dag är föreskriven på förordningsnivå (8 § PUF). Vi anser dock att de undantag vi föreslår för myndigheters behandling av känsliga personuppgifter bör regleras i lag. Vi bedömer i och för sig inte att de nu föreslagna undantagen är av sådant slag att de måste regleras i lag enligt 2 kap. 6 och 20 §§ regeringsformen. Bestämmelsen i 8 kap. 2 § 2 regeringsformen ger vidare möjlighet att meddela undantag från förbudet mot behandling av känsliga personuppgifter med stöd i ett bemyndigande, se avsnittet nedan. Med tanke på att de undantag vi föreslår för myndigheternas behandling av känsliga personuppgifter gäller generellt, utan begränsning till viss typ av verksamhet eller vissa typer av ärenden, är det ändå lämpligt att regleringen får lagform.

Bemyndigande som möjliggör ytterligare undantag

Bemyndigandet i 20 § PUL har som nämnts ovan utnyttjats i flera fall för att föreskriva i förordning att behandling för viktiga allmänna intressen får ske utöver undantaget för myndigheters behandling i 8 § PUF, bland annat för att reglera privata aktörers behandling av känsliga personuppgifter. Det kommer att finnas ett fortsatt behov av att i förordning kunna föreskriva undantag för viktiga allmänna intressen för vissa tydligt avgränsade ändamål eller för vissa särskilda verksamheter, utöver de generella undantag för myndigheter som vi föreslår. På grund av att den så kallade missbruksregeln i 5 a § PUL inte längre kommer att kunna utgöra stöd för behandling när förordningen börjar tillämpas, kommer sannolikt behovet av ytterligare undantag att öka.

Frågan är då om ett bemyndigande krävs för att åstadkomma en sådan möjlighet. I motiven till personuppgiftslagen har det ansetts att reglering som rör i vilka konkreta fall viktiga allmänna intressen gör det befogat att känsliga personuppgifter behandlas trots det generella förbudet mot behandling av sådana uppgifter, är sådana offentligrättsliga föreskrifter som tillhör det primära lagområdet men som kan meddelas efter delegation enligt nuvarande 8 kap. 2 § 2 och 3 § regeringsformen.¹⁸

Vi instämmer i den bedömning som har gjorts tidigare. Eftersom ett principiellt förbud mot behandling av känsliga personuppgifter gäller till skydd för enskilda, innebär en reglering som möjliggör behandling av just känsliga personuppgifter enligt vår mening ett sådant ingrepp i enskildas personliga förhållanden som enligt 8 kap. 2 § 2 regeringsformen ska ha stöd i ett bemyndigande. Några problem med det befintliga bemyndigandet till regeringen har inte framkommit. Vi föreslår därför att ett bemyndigande för regeringen att föreskriva om undantag förs in i dataskyddslagen. Eftersom regeringen hittills inte har sett anledning att utnyttja möjligheten i 20 § PUL att bemyndiga Datainspektionen att meddela föreskrifter och något behov av sådan vidaredelegation inte har framkommit, föreslår vi ingen sådan möjlighet.

När nya undantag övervägs med stöd av bemyndigandet måste en noggrann bedömning göras av om lagform ändå krävs enligt 2 kap. 6 och 20 §§ regeringsformen. Det måste också säkerställas att förordningens krav i övrigt, bland annat när det gäller skyddsåtgärder, är uppfyllda.

10.7 Hälsa- och sjukvård och social omsorg

10.7.1 Gällande rätt

Dataskyddsdirektivets undantag för behandling av känsliga personuppgifter på hälso- och sjukvårdsområdet (artikel 8.3) har följande lydelse.

Punkt 1 gäller inte när behandlingen av uppgifterna är nödvändig med hänsyn till förebyggande hälso- och sjukvård, medicinska diagnoser, vård eller behandling eller administration av hälso- eller sjukvård eller

¹⁸ Prop. 1997/98:44 s. 59 f och SOU 1997:39 s. 328.

när dessa uppgifter behandlas av någon som är yrkesmässigt verksam på hälso- och sjukvårdsområdet och som enligt nationell lagstiftning eller bestämmelser som antagits av behöriga nationella organ är underkastad tystnadsplikt eller av en annan person som är ålagd en liknande tystnadsplikt.

Bestämmelsen har genomförts i 18 § PUL. I första stycket stadgas att känsliga personuppgifter får behandlas för hälso- och sjukvårdsändamål, om behandlingen är nödvändig för förebyggande hälso- och sjukvård, medicinska diagnoser, vård eller behandling, eller administration av hälso- och sjukvård. Bestämmelsen anses täcka nästan all behandling av personuppgifter som förekommer inom hälso- och sjukvårdsområdet. Bland annat har internationellt folkhälsoarbete, kvalitetshöjande behandling av personuppgifter, debitering av avgifter och tillsyn över hälso- och sjukvård ansetts omfattas av bestämmelsen.

I andra stycket första meningen samma paragraf stadgas att den som är yrkesmässigt verksam inom hälso- och sjukvårdsområdet och har tystnadsplikt även får behandla sådana känsliga personuppgifter som omfattas av tystnadsplikten. Detsamma gäller enligt andra meningen i samma stycke den som är underkastad en liknande tystnadsplikt och som har fått känsliga personuppgifter från verksamhet inom hälso- och sjukvårdsområdet. I bestämmelsen uppställs inget krav på att uppgifterna ska behandlas för hälso- och sjukvårdsändamål. Det krav som ställs i praktiken är alltså i stället att den person som behandlar uppgifterna omfattas av tystnadsplikt enligt 25 kap. 1 § OSL, eller enligt 12 § patientsäkerhetslagen (2010:659), antingen direkt eller genom att tystnadsplikten överförs i sådana fall som avses i 11 kap. OSL. Den svenska implementeringen av direktivet genom 18 § andra stycket PUL har fått kritik för att den innebär en väsentlig utvidgning i förhållande till direktivet. Detta kan bero på att den svenska versionen av direktivet är felöversatt. Enligt de engelsk- och franskspråkiga versionerna av direktivet gäller kravet på tystnadsplikt utöver kravet på att behandlingen ska ske för de särskilt angivna hälso- och sjukvårdsändamålen.¹⁹

Bestämmelsen i 18 § andra stycket andra meningen PUL om den som har fått uppgifter från en verksamhet inom hälso- och sjukvårdsområdet infördes efter remissynpunkter för att genomföra direktivets bestämmelse om behandling av en annan person som är ålagd en

¹⁹ SOU 2006:82 s. 175 och Rynning, Förvaltningsrättslig tidskrift 2003 s. 112.

liknande tystnadsplikt som yrkesverksamma på hälso- och sjukvårdsområdet. Syftet var att reglera situationer när känsliga personuppgifter lämnas av en myndighet inom hälso- och sjukvården till forskningsverksamhet eller verksamhet för tillsyn eller revision hos annan myndighet.²⁰

I dag regleras behandling av personuppgifter inom hälso- och sjukvården framför allt i patientdatalagen. Behandling av uppgifter om känsliga personuppgifter i den verksamheten anses ske med stöd av ändamålsbestämmelserna i 2 kap. 4 och 7 §§ nämnda lag.²¹ I 2 kap. 8 § patientdatalagen finns också en bestämmelse som reglerar möjligheterna att använda känsliga personuppgifter som sökbegrepp. Patientdatalagen reglerar inte behandling av känsliga personuppgifter som sker hos tillsynsmyndigheterna på hälso- och sjukvårdsområdet, dvs. exempelvis Datainspektionen, Socialstyrelsen och Inspektionen för vård och omsorg. Sådan behandling sker direkt med stöd av 18 § PUL.

10.7.2 Överväganden och förslag

Utredningens förslag: Känsliga personuppgifter ska få behandlas för sådana ändamål relaterade till hälso- och sjukvård samt social omsorg som avses i dataskyddsförordningen, under förutsättning att förordningens krav på tystnadsplikt är uppfyllt.

I artikel 9.2 h i dataskyddsförordningen har några ytterligare verksamhetstyper lagts till den uppräknade av verksamheter som anges i direktivets motsvarande artikel i hälso- och sjukvårdsundantaget, nämligen yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet och social omsorg. Sannolikt omfattar tillägget avseende arbetskapacitet behandling av uppgifter relaterade till sjukskrivning och rehabilitering på arbetet och begreppet social omsorg snarast uppgifter som utförs av socialtjänsten.

Vissa justeringar i artikeltexten i övrigt har också gjorts. Begreppet vård har ersatts med tillhandahållande av hälso- och sjukvård och begreppet administration av hälso- och sjukvård har ersatts med för-

²⁰ Prop. 1997/98:44 s. 125.

²¹ Prop. 2007/08:126 s. 63 och 230 f.

valtning av hälso- och sjukvårdstjänster och deras system. Av dataskyddsförordningens skäl 53 framgår att avsikten är att begreppet förvaltning av hälso- och sjukvårdstjänster ska tolkas vitt och bland annat inbegripa behandling som utförs av centrala nationella hälsovårdsmyndigheter samt vid tillsyn över hälso- och sjukvård och social omsorg. Dessutom har direktivets formulering att behandlingen ska vara nödvändig med hänsyn till sådan verksamhet som omnämns i artikeln, bytts ut till att behandlingen ska vara nödvändig av skäl som hör samman med sådan verksamhet.

Av artikel 9.3, som är direkt tillämplig, framgår att behandling av känsliga personuppgifter som avses i artikel 9.2 h får utföras av, eller under ansvar av, personer som omfattas av tystnadsplikt enligt unionsrätten, medlemsstaternas nationella rätt eller bestämmelser som fastställs av nationella behöriga organ. I artikeln tydliggörs också att sådan behandling ska ske för de ändamål som nämns i artikel 9.2 h. Förordningens reglering tycks alltså sammanfattningsvis innebära att all behandling enligt artikel 9.2 h förutsätter såväl tystnadsplikt som att behandlingen sker för de särskilt angivna hälso- och sjukvårdsrelaterade ändamålen.

Det är av stor vikt att förutsättningarna för att behandla känsliga personuppgifter för hälso- och sjukvårdsändamål är reglerade på ett så tydligt sätt som möjligt. Det finns sannolikt även fortsättningsvis ett behov av att detaljreglera de närmare förutsättningarna för behandling av personuppgifter på dessa områden, även känsliga personuppgifter, i sektorsspecifik författning. Det är dock inte självklart att sådana författningar kan och bör reglera även exempelvis tillsynsmyndigheternas behandling. Det har inte framkommit annat under utredningens arbete än att den nuvarande regleringen behövs. Vi menar därför att ett grundläggande undantag när det gäller behandling av känsliga personuppgifter i verksamhet på hälso- och sjukvårdsområdet och inom social omsorg även fortsättningsvis bör finnas i generell reglering, dvs. i dataskyddslagen.

Vi föreslår att den befintliga regleringen i 18 § första stycket PUL används som utgångspunkt, men att ordalydelsen anpassas till de tillägg och justeringar som har gjorts i förordningstexten i artikel 9.2 h jämfört med direktivtexten. Känsliga personuppgifter ska alltså få behandlas om behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagno-

ser, tillhandahållande av hälso- och sjukvård eller behandling, social omsorg samt förvaltning av social omsorg, hälso- och sjukvårdstjänster och deras system.

Det framgår enligt vår mening tydligt av förordningstexten i artikel 9.2 h och artikel 9.3 att all behandling måste ske för de närmare specificerade hälso- och sjukvårdsrelaterade ändamål som nämns i artikel 9.2 h, och att sådan behandling bara får ske av eller under ansvar av en person som omfattas av tystnadsplikt enligt gällande rätt. Eftersom artikel 9.3 i förordningen är direkt tillämplig får den närmare innebörden av kravet på tystnadsplikt ytterst uttolkas av EU-domstolen. I Sverige regleras tystnadsplikt inom de områden som täcks av artikeln i bland annat 25 och 26 kap. OSL och 6 kap. 12–16 §§ patientsäkerhetslagen.

Enligt förordningens skäl 53 omfattas behandling av känsliga personuppgifter inom tillsyn över hälso- och sjukvård av artikel 9.2 h. Därmed bör enligt vår bedömning den behandling som åsyftas i 18 § andra stycket PUL kunna omfattas av ordalydelsen i artikel 9.2 h och 9.3 i förordningen.

10.8 Folkhälsa

10.8.1 Gällande rätt

Något särskilt undantag från förbudet mot behandling av känsliga personuppgifter i fråga om behandling för folkhälsoändamål finns inte i dataskyddsdirektivet. I skäl 34 i direktivet nämns i stället folkhälsa som ett sådant område där ett undantag kan vara motiverat av hänsyn till viktiga allmänna intressen. Internationellt folkhälsoarbete har i svensk rätt ansetts falla in under formuleringen förebyggande hälsovård i 18 § PUL, dvs. det så kallade hälso- och sjukvårdsundantaget.²²

²² Prop. 2005/06:215 s. 47.

10.8.2 Överväganden

Utredningens bedömning: Något undantag för behandling av känsliga personuppgifter på folkhälsoområdet bör inte införas i dataskyddslagen.

I förordningens artikel 9.2 i finns ett särskilt undantag från förbudet att behandla känsliga personuppgifter som tar sikte på behandling som är nödvändig av skäl av allmänt intresse på folkhälsoområdet, såsom behovet av att säkerställa ett skydd mot allvarliga gränsöverskridande hot mot hälsan eller säkerställa höga kvalitets- och säkerhetsnormer för vård och läkemedel eller medicintekniska produkter. Artikelns innehåller en hänvisning till nationell rätt och ett krav på att lämpliga och specifika åtgärder fastställs för att skydda den registrerade fri- och rättigheter. Tystnadsplikt framhålls särskilt som en sådan åtgärd som ska fastställas.

I förordningens skäl 54 anges att termen folkhälsa bör tolkas i enlighet med förordning 1338/2008 om gemenskapsstatistik om folkhälsa och hälsa och säkerhet i arbetet.²³ Den definition som anges där är mycket vid och omfattar ”alla aspekter som rör hälsosituationen, dvs. allmänhetens hälsotillstånd, inbegripet sjuklighet och funktionshinder, hälsans bestämningsfaktorer, hälso- och sjukvårdsbehov, resurser inom hälso- och sjukvården, tillhandahållande av och allmän tillgång till hälso- och sjukvård, utgifter för och finansiering av hälso- och sjukvården samt dödsorsaker”.

Folkhälsoarbete anses i Sverige vara tvärsektoriellt och involverar såväl Folkhälsomyndighetens arbete som arbete inom kommuner, landsting och länsstyrelser. Hos Folkhälsomyndigheten ligger en stor del av arbetet med att säkerställa ett skydd mot allvarliga gränsöverskridande hot mot hälsan.²⁴ Uppgiften att säkerställa kvalitets- och säkerhetsnormer för vård och läkemedel eller medicintekniska produkter ligger i Sverige främst hos Läkemedelsverket och Socialstyrelsen.

Det är oklart om förordningens undantag på folkhälsoområdet egentligen innebär ökade möjligheter att behandla känsliga person-

²³ Europaparlamentets och rådets förordning (EG) nr 1338/2008 av den 16 december 2008 om gemenskapsstatistik om folkhälsa och hälsa och säkerhet i arbetet.

²⁴ 2 § förordningen (2013:1021) med instruktion för Folkhälsomyndigheten.

uppgifter jämfört med direktivet. Undantaget infördes under förordningens behandling i rådet, och fanns alltså inte med i kommissionens ursprungliga förslag. Något liknande förslag har inte heller framförts av Europaparlamentet eller den europeiska datatillsynsmannen under arbetet med förordningen.

Behandling av känsliga personuppgifter på folkhälsoområdet sker i dag antingen med stöd av undantaget avseende behandling inom hälso- och sjukvården eller med stöd av undantaget som avser behandling av hänsyn till ett viktigt allmänt intresse. En stor del av den verksamhet som bedrivs på folkhälsoområdet i Sverige innebär till exempel behandling för statistikändamål, och har ansetts kunna ske med stöd av 19 § PUL, som i sin tur har införts med stöd av direktivets undantag av hänsyn till ett viktigt allmänt intresse. Det har inte framkommit att Folkhälsomyndigheten, Läke medelsverket, Socialstyrelsen eller kommuner och landsting har upplevt att stöd saknas för den behandling av känsliga personuppgifter som måste ske inom nationellt eller internationellt folkhälsoarbete.

Med det krav som finns i artikel 9.2 i på att *specifika* skyddsåtgärder ska fastställas bedömer vi att undantaget måste genomföras i nationell rätt för att vara tillämpligt. Vår bedömning är emellertid att den behandling av känsliga personuppgifter som är nödvändig på folkhälsoområdet i många fall kan ske med stöd av de undantag vi föreslår avseende behandling för viktiga allmänna intressen, för statistiska ändamål samt på hälso- och sjukvårdsområdet. Vi bedömer därför att något behov inte finns av ett särskilt undantag i dataskyddslagen för behandling av känsliga personuppgifter på folkhälsoområdet. Om det finns behov för någon av de myndigheter som arbetar inom folkhälsoområdet att ha ytterligare möjligheter att behandla känsliga personuppgifter, bör detta enligt vår mening i första hand övervägas i sektorsspecifik reglering, där en bedömning av befintligt sekretesskydd och behov av andra specifika skyddsåtgärder kan bedömas för varje myndighet för sig.

11 Personuppgifter som rör lagöverträdelser

11.1 Vårt uppdrag

Enligt kommittédirektiven ska utredningen analysera i vilken utsträckning det bör införas regler i den kompletterande regleringen som tillåter behandling av uppgifter om lagöverträdelser som inte sker under kontroll av en myndighet. En lämplig utgångspunkt för en sådan analys är enligt direktiven den befintliga regleringen om behandling för forskningsändamål och den delegerade föreskriftsrätten i personuppgiftslagen.

Som framgår av avsnitt 2.2 har vi i samråd med Forskningsdatautredningen konstaterat att samtliga frågor rörande behandling av personuppgifter för forskningsändamål bör behandlas i ett samlat sammanhang och att Forskningsdatautredningen är bäst lämpad att göra den analys och de överväganden som krävs. Vi behandlar därför inte frågan om behandling av uppgifter om lagöverträdelser för forskningsändamål.

Våra överväganden och förslag när det gäller behandling av personuppgifter som rör lagöverträdelser för arkivändamål av allmänt intresse finns i avsnitt 14.

11.2 Gällande rätt

Uppgifter om lagöverträdelser och liknande uppgifter tillhör inte de särskilda kategorier av personuppgifter som omfattas av förbudet i artikel 8.1 i dataskyddsdirektivet, men anses ändå vara en kategori personuppgifter som förtjänar särskilt skydd.¹

¹ Uppgifter om fällande domar jämföras med känsliga personuppgifter i artikel 6 i dataskyddskonventionen.

I direktivet regleras behandling av uppgifter om lagöverträdelser, brottmålsdomar eller säkerhetsåtgärder i artikel 8.5. Där stadgas att sådan behandling endast får utföras under kontroll av en myndighet eller med stöd av nationella bestämmelser som innehåller lämpliga och specifika skyddsåtgärder. Det stadgas också att ett fullständigt register över brottmålsdomar bara får föras under kontroll av en myndighet. Enligt artikelns andra stycke får medlemsstaterna föreskriva att uppgifter som rör administrativa sanktioner eller avgöranden i tvistemål också ska behandlas under kontroll av en myndighet.

Bestämmelsen har genomförts i svensk rätt genom 21 § PUL. Enligt paragrafens första stycke gäller ett förbud för andra än myndigheter att behandla personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden. Som framgår av 21 § PUL har direktivets formulering ”under kontroll av en myndighet” tolkats som att ett förbud ska gälla för andra än myndigheter att behandla uppgifter om lagöverträdelser.²

I 21 § tredje och fjärde styckena PUL finns bemyndiganden för regeringen eller den myndighet regeringen bestämmer att meddela föreskrifter eller beslut i enskilda fall om undantag från förbudet för enskilda att behandla sådana uppgifter. Datainspektionen har med stöd av ett bemyndigande i 9 § PUF meddelat sådana föreskrifter bland annat för att möjliggöra behandling av enstaka uppgifter som är nödvändig för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras i ett enskilt fall, liksom behandling av enstaka uppgifter som är nödvändig för att anmälningsskyldighet enligt lag ska kunna fullgöras.³

Begreppet överträdelser i direktivet har bedömts innebära att det ska vara fråga om överträdelser som är straffsanktionerade, vilket uttryckts i lagtexten som lagöverträdelser som innefattar brott.⁴ Det är inte helt klart i vilken utsträckning uppgifter som rör misstankar om brott omfattas. Datalagskommittén menade att uppgifter om faktiska iakttagelser om en persons handlande inte rimligen kunde anses som uppgifter om lagöverträdelser i alla fall.⁵ Högsta förvaltningsdomstolen har dock uttalat att behandling av uppgifter om fordon som förekommit i samband

² SOU 1997:39 s. 382 och prop. 1997/98:44 s. 74 f.

³ DIFS 2010:1, Datainspektionens föreskrifter om ändring av Datainspektionens föreskrifter (DIFS 1998:3) om undantag från förbudet för andra än myndigheter att behandla personuppgifter om lagöverträdelser m.m.

⁴ SOU 1997:39 s. 383.

⁵ SOU 1997:39 s. 383.

med obetalda tankningar ska ses som en behandling av personuppgifter om lagöverträdelser.⁶

Uttrycken straffprocessuella tvångsmedel och administrativa frihetsberövanden i 21 § PUL är avsedda att motsvara uttrycken säkerhetsåtgärder och administrativa sanktioner i direktivet.⁷ Med administrativa frihetsberövanden avses exempelvis frihetsberövanden enligt lagen om psykiatrisk tvångsvård, lagen om vård av missbrukare och lagen med särskilda bestämmelser om vård av unga, liksom uppgifter om frihetsberövande av utlänningar enligt 10 kap. utlänningslagen (2005:716). Möjligheten att reglera uppgifter om avgöranden i tvistemål har inte utnyttjats. Den reglering som fanns i kreditupplysningslagen ansågs tillräcklig.⁸

11.3 Dataskyddsförordningen

I förordningen används delvis andra formuleringar än i dataskyddsdirektivet. Artikel 10 lyder som följer.

Behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder enligt artikel 6.1 får endast utföras under kontroll av myndighet eller då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs. Ett fullständigt register över fällande domar i brottmål får endast föras under kontroll av en myndighet.

Inledningsvis kan konstateras att tillämpningsområdet begränsats till enbart fällande brottmålsdomar. Behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder får enligt artikeln utföras under kontroll av myndighet. Begreppet ”under kontroll av myndighet” definieras inte. Det används också i sista meningen i artikel 10, där det stadgas att fullständiga register över fällande domar i brottmål endast får föras under sådan kontroll. Utöver behandling under kontroll av en myndighet kan ytterligare behandling tillåtas i unionsrätten eller medlemsstaternas nationella rätt om lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs.

⁶ HFD 2016 ref. 8.

⁷ Prop. 1997/98:44 s. 74 f.

⁸ Prop. 1997/98:44 s. 75.

Begreppet lagöverträdelser har ersatts med överträdelser i den svenska språkversionen. I den engelska versionen används begreppet *criminal convictions and offences* och i den franska versionen *condamnations pénales et aux infractions*. Inga skäl finns i förordningen, som skulle kunna klargöra om avsikten är någon saklig skillnad jämfört med direktivet. Såväl den engelska som den franska textversionen av förordningen talar för att det som avses med termen överträdelser är överträdelser som innefattar brott.

Innebörden av det tillägg i form av en hänvisning till artikel 6.1 som införts i artikeltexten är oklar, men kan möjligen tolkas som en erinran om att behandlingen i fråga måste uppfylla kraven i nämnda artikel i förordningen.

En betydande skillnad i förordningen jämfört med direktivet är att någon möjlighet för medlemsstaterna att på denna grund begränsa behandlingen av personuppgifter om avgöranden i tvistemål och administrativa sanktioner inte finns.

11.4 Överväganden och förslag

Utredningens förslag: Personuppgifter som rör fällande domar i brottmål, lagöverträdelser som innefattar brott eller straffprocessuella tvångsmedel ska få behandlas av myndigheter. Datainspektionen ska i enskilda fall få besluta om att tillåta sådan behandling för andra än myndigheter.

Vissa bestämmelser som tillåter andra än myndigheter att behandla motsvarande uppgifter ska föras in i förordningen till dataskyddslagen. Regeringen eller, efter bemyndigande från regeringen, Datainspektionen ska få meddela ytterligare sådana föreskrifter.

Utredningens bedömning: Det finns inte stöd i förordningen för att föreskriva ett förbud mot behandling av personuppgifter om administrativa frihetsberövanden.

De delar av artikel 10 som rör behandling av uppgifter om fällande domar i brottmål, överträdelser och därmed sammanhängande säkerhetsåtgärder under kontroll av en myndighet är direkt tillämpliga. Det är emellertid av stor vikt att regleringen i artikel 10, även vad avser myndigheters behandling, tydliggörs så långt möjligt i nationell rätt. Behand-

ling av sådana uppgifter torde allmänt anses som integritetskänslig, och risken för missbruk, exempelvis genom otillbörlig spridning på internet, framstår som stor. Behandling i strid med artikel 10 kommer enligt vårt förslag vidare att kunna föranleda att sanktionsavgifter påförs (se avsnitt 18.6.4).

Förordningens skäl 8 ger uttryck för att medlemsstaterna får införliva delar av förordningen i nationell rätt, om det krävs för att göra de nationella bestämmelserna begripliga för de personer de tillämpas på. Vi menar att ett sådant införlivande skulle fylla en viktig funktion när det gäller myndigheters behandling av uppgifter om lagöverträdelser, bland annat för att tydliggöra att myndigheter inte behöver uttryckligt stöd i föreskrifter eller särskilda beslut för att få behandla uppgifter om lagöverträdelser. Vår bedömning är därför att första ledet i förordningens artikel 10 bör införlivas i svensk rätt.

Begreppet överträdelser bedömer vi som nämnts ovan som likvärdigt med direktivets begrepp lagöverträdelser, vilket i personuppgiftslagen tolkades som lagöverträdelser som innefattar brott. Detta överensstämmer också med den engelska och franska versionen av förordningen. För att inte riskera en alltför vid tolkning av ordet överträdelser i svensk rätt bör därför begreppet lagöverträdelser som innefattar brott användas även fortsättningsvis. I vilken utsträckning misstankar om brott omfattas av begreppet överträdelser i förordningen framgår inte av artikeltext eller skäl. I avvaktan på klargörande EU-rättslig praxis bedömer vi att misstankar om brott bör omfattas i samma utsträckning som de gör enligt personuppgiftslagen.

Begreppet säkerhetsåtgärder bedömdes i nu aktuellt avseende som likvärdigt med straffprocessuella tvångsmedel vid genomförandet av direktivet.⁹ Slutsatsen motiverades inte närmare, men ligger språkligt väl i linje med i vart fall den engelska språkversionen av förordningen. Eftersom säkerhetsåtgärder används i en annan betydelse på flera håll i förordningen – exempelvis i artiklarna 30.1 g och 35.7 d – anser vi att begreppet straffprocessuella tvångsmedel bör användas i författningstexten även fortsättningsvis.

Som nämnts ovan är innebörden av begreppet under kontroll av en myndighet inte helt klar. Vår bedömning är att det inte kan avse enbart ett krav på att den personuppgiftsansvarige allmänt står under tillsyn av en myndighet. All behandling av personuppgifter enligt förordningen är

⁹ Prop. 1997/98:44 s. 74.

föremål för tillsyn såväl på nationell som på EU-nivå. Eftersom förande av regelrätta register över fällande domar i brottmål enligt förordningen får ske under kontroll av en myndighet kan begreppet rimligen inte tolkas alltför vitt.

Vi menar att det finns goda skäl att anta att uttrycket framför allt är avsett att begränsa rätten att behandla uppgifter till behandling av uppgifter som utförs av myndigheter och att detta tydligt bör framgå av den svenska regleringen. Liksom när det gäller behandling av känsliga personuppgifter förtjänar det att påpekas i detta sammanhang att all behandling av personuppgifter, även behandling av uppgifter om lagöverträdelse hos myndigheter, måste leva upp till förordningens krav i det enskilda fallet, exempelvis de grundläggande kraven på behandling i artikel 5. Att det tydliggörs i dataskyddslagen att myndigheter generellt tillåts behandla uppgifter om lagöverträdelse innebär alltså inte att sådan behandling alltid är tillåten i det enskilda fallet.

Uttrycket "under kontroll av myndighet" utesluter inte enligt sin ordalydelse att behandling får ske utanför myndighets sfären. För sådan behandling kan den kontroll av myndighet som förutsätts enligt förordningen enligt vår mening upprätthållas genom att den får ske med stöd av särskilda beslut som fattas av tillsynsmyndigheten. Besluten bör lämpligen förenas med villkor såsom återkallelseförbehåll, tidsbegränsningar eller krav på återrapportering. Behandlingen blir därmed föremål för särskilda tillsynsinsatser, och kan således anses ske under kontroll av en myndighet. Ett beslut om att tillåta behandling av uppgifter om lagöverträdelse i enskilda fall bör, mot bakgrund av uppgifternas integritetskänsliga karaktär, bara meddelas om intresset av sådan behandling väger tyngre än de registrerades intresse av att behandling inte sker. Vidare innebär inte ett sådant beslut att den personuppgiftsansvarige fritas från sitt ansvar att se till att behandlingen i det enskilda fallet lever upp till förordningens krav, exempelvis de grundläggande kraven på behandling i artikel 5.

Dataskyddsförordningen ger ett alternativ till att behandlingen får ske under kontroll av myndighet, nämligen att behandlingen på annan grund är tillåten enligt nationell rätt förutsatt att lämpliga skyddsåtgärder fastställs. Enligt vår mening är det inte lämpligt eller ens möjligt att i den generella lagen föreskriva närmare vilken reglering som skulle behövas på detta område. I stället bör det övervägas i särskild ordning där behovet särskilt kan analyseras från fall till fall. En lämplig lösning är därför ett bemyndigande för regeringen och vidare till Datainspektionen att meddela föreskrifter om i vilka fall andra än myndigheter får behandla

uppgifter om lagöverträdelse. För att sådana ska vara förenliga med förordningen förutsätts att lämpliga skyddsåtgärder fastställs i föreskrifterna.

Sammanfattningsvis menar vi att bestämmelser som så långt dataskyddsförordningen medger motsvarar de som finns i 21 § första, tredje och fjärde stycket PUL bör föras in i dataskyddslagen. Som framgått ovan föreslår vi emellertid en reglering som inte längre uttrycks som ett generellt förbud med möjligheter till undantag, på det sätt som 21 § PUL har utformats. Denna skillnad mot personuppgiftslagen sammanhänger med den något ändrade tolkningen av begreppet ”under kontroll av myndighet”, som vi alltså menar bör ges en självständig betydelse när det gäller möjligheten att behandla uppgifter om lagöverträdelse utanför myndighetssfären. I ljuset av detta delvis förändrade synsätt framstår det enligt vår mening som naturligt att utrymmet för att tillåta andra än myndigheter att behandla uppgifter om lagöverträdelse blir något mindre begränsat än tidigare. I detta sammanhang bör nämnas att behovet av särskilda föreskrifter eller beslut torde öka som en följd av att den så kallade missbruksregeln i 5 a § PUL försvinner.

Vi bedömer till exempel att det kan finnas behov av tydligare stöd för behandling av uppgifter om lagöverträdelse i brottsanmälningar och i viss advokatverksamhet. Det har under utredningen också framkommit behov av en föreskrift som tillåter behandling av sådana uppgifter om lagöverträdelse som måste behandlas till följd av rättsliga förpliktelser. I det sammanhanget har det nämnts att sådana förpliktelser exempelvis skulle kunna förekomma i reglering som syftar till att bekämpa t.ex. korruption, terrorism, finansiering av grov brottslighet och olämplig spridning av vapentechnologi. Vi har visserligen inte haft möjlighet att närmare utreda i vilken utsträckning sådana rättsliga förpliktelser redan förekommer och om de i så fall står i strid med dataskyddsförordningens och de föreslagna bestämmelserna i dataskyddslagen om behandling av personuppgifter som rör lagöverträdelse. Vi kan dock konstatera att den typen av normkonflikt skulle vara problematisk. Mot denna bakgrund föreslår vi att bestämmelserna i 1 § d) och e) i Datainspektionens föreskrifter (DIFS 1998:3) om undantag från förbudet för andra än myndigheter att behandla personuppgifter om lagöverträdelse m.m., i den lydelse som fastställts genom DIFS 2010:1, bör utvidgas något och föras in i förordningen till dataskyddslagen, tillsammans med en ny bestämmelse som tillåter nödvändig behandling av motsvarande uppgifter vid polisanmälningar om misstanke om brott.

Som framgått ovan finns det inte stöd i förordningens artikel 10 för något förbud motsvarande det som nu gäller för andra än myndigheter att behandla uppgifter om administrativa frihetsberövanden. Vissa sådana uppgifter skulle kunna omfattas av förbudet mot att behandla känsliga personuppgifter i artikel 9.1, exempelvis om de också avslöjar uppgifter om etniskt ursprung eller psykisk ohälsa. Regleringen i artiklarna 5 och 6 innebär vidare att privata subjekt i praktiken ändå torde ha begränsade möjligheter att behandla sådana uppgifter.

12 Personnummer och samordningsnummer

12.1 Vårt uppdrag

I 22 § PUL finns en särskild bestämmelse om när personnummer eller samordningsnummer får behandlas. Bestämmelsen innebär att uppgifter om personnummer eller samordningsnummer får behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Enligt dataskyddsförordningen får medlemsstaterna fastställa särskilda villkor för sådan behandling. Vårt uppdrag i denna del innebär att vi ska överväga om det även fortsättningsvis bör finnas sådana särskilda villkor för behandling av personnummer eller samordningsnummer.

12.2 Gällande rätt

22 § PUL har genomförts med stöd av artikel 8.7 i dataskyddsdirektivet, där det föreskrivs att medlemsstaterna ska bestämma på vilka villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas. Bestämmelsen behöver inte tillämpas vid sådan behandling av personuppgifter i ostrukturerat material som avses i 5 a § PUL. En motsvarande bestämmelse om användningen av personnummer fanns i 7 § andra stycket datalagen. Den bestämmelsen fördes i princip oförändrad över till personuppgiftslagen.

De villkor som uppställs i paragrafen innebär att uppgifter om personnummer eller samordningsnummer får behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

För en personuppgiftsansvarig som inte fått samtycke till behandling av personnummer eller samordningsnummer innebär bestämmelsen att denne själv måste göra den intresseavvägning som framgår av bestämmelsen. Den personuppgiftsansvarige torde också ha bevisbördan för att det finns sådana omständigheter som gör att uppgifter om personnummer eller samordningsnummer får behandlas.

Exempel på hur lagstiftaren har gjort motsvarande avvägningar finns i flera av de lagstiftningsärenden rörande sektorspecifika författningar där en hänvisning till 22 § PUL har tagits in. Med hänsyn framför allt till vikten av en säker identifiering har det exempelvis ansetts motiverat att behandla personnummer i polisens, Migrationsverkets och domstolarnas verksamhet, liksom i vårdregister, rättspsykiatriska forskningsregister och inom socialtjänsten.¹

I 50 § c PUL finns ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer, dvs. Datainspektionen enligt 16 § PUF, att meddela närmare föreskrifter om i vilka fall användning av personnummer är tillåten. Några sådana föreskrifter har inte meddelats av Datainspektionen. Det är däremot relativt vanligt med sektorsspecifika förordningsbestämmelser om behandling av personnummer och samordningsnummer, såsom till exempel 3 § 1 förordningen (2002:623) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten. Det är dock inte helt klart om den bestämmelsen har ansetts stödja sig på bemyndigandet i 50 § c PUL, eller om den har föreskrivits med stöd av regeringens restkompetens enligt 8 kap. 7 § 2 regeringsformen.

12.3 Dataskyddsförordningen

Dataskyddsförordningen ger medlemsstaterna möjlighet att bestämma särskilda villkor för när ett nationellt identifikationsnummer eller annat vedertaget sätt för identifiering får behandlas (artikel 87). Enligt förordningen ska villkoren i sådana fall säkerställa att identifikationsuppgifterna bara får användas med iakttagande av lämpliga skyddsåtgärder för de registrerades fri- och rättigheter. Något uttryckligt sådant krav fanns inte enligt dataskyddsdirektivet.

¹ Prop. 1997/98:108 s. 73 f., prop. 1998/99:72 s. 44, prop. 2000/01:80 s. 144, prop. 2009/10:85 s. 84, prop. 2014/15:148 s. 51 och prop. 2015/16:65 s. 49 f.

12.4 Överväganden och förslag

Utredningens förslag: Uppgifter om personnummer eller samordningsnummer ska få behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Regeringen ska få meddela ytterligare föreskrifter om behandling av uppgifter om personnummer och samordningsnummer.

Den nuvarande regleringen i 22 § PUL ger uttryck för att behandlingen av personnummer och samordningsnummer bör vara restriktiv och föregås av en intresseavvägning mellan behovet av behandlingen och de integritetsrisker som den innebär.

Dataskyddsförordningen uppställer inget krav på reglering i detta avseende, men om medlemsstaterna bestämmer särskilda villkor för sådan behandling måste lämpliga skyddsåtgärder för de registrerades fri- och rättigheter enligt förordningen säkerställas. Det finns inga uttalanden i skälen som konkretiserar vilken typ av skyddsåtgärder det bör vara frågan om. Sannolikt kan kraven på skyddsåtgärder inte ställas särskilt högt, eftersom det är upp till medlemsstaterna själva att bedöma om några särskilda villkor ska införas över huvud taget. I denna del ges alltså medlemsstaterna ett stort utrymme att själva bedöma vilka skyddsåtgärder som behövs.

Personnummer och samordningsnummer har inte bedömts som känsliga personuppgifter i förordningens mening, men har ändå getts en särställning genom att medlemsstaterna medgetts möjlighet att införa särskilda villkor för behandlingen.

Regeringen har i äldre förarbeten uttalat att själva personnumret inte i sig är en integritetskränkande uppgift, men att viss användning av det, såsom samkörning av register och liknande, kan uppfattas som integritetskränkande. Regeringen har också uttalat att "onödig" användning ska betraktas som ett integritetsintrång.² Kammarätten i Stockholm har nyligen bedömt att integritetsintresset väger tungt vid mer omfattande behandling av personnummer.³

² Prop. 1990/91:60 s. 69.

³ Kammarättens i Stockholm dom av den 11 mars 2016 i mål nr 6352-15. Högsta förvaltningsdomstolen har beslutat att inte meddela prövningstillstånd, beslut den 12 oktober 2016 i mål nr 1684-16.

Vår bedömning mot bakgrund av ovanstående är att en särreglering av personnummer och samordningsnummer i dataskyddslagen är motiverad. Den nuvarande lydelsen i 22 § PUL, som innebär att en intresseavvägning ska ske, ligger väl i linje med förordningens intentioner. Det har inte framkommit att regleringen har mötts av kritik eller annars inte fungerat. Tvärtom har den i lagstiftningsärenden under de senaste åren bedömts vara flexibel och väl avpassad för att förhindra omotiverad behandling av personnummer och samordningsnummer.⁴ Vi bedömer därför att en bestämmelse motsvarande den i 22 § PUL bör införas i dataskyddslagen.

Den nationella reglering som åsyftas i artikel 87 i dataskyddsförordningen kan enligt förordningens skäl 41 även beslutas i förordnings- eller föreskriftsform. Som nämnts finns i dag bestämmelser på förordningsnivå som reglerar behandlingen av personnummer och samordningsnummer i sektorsspecifika författningar. Vi bedömer att det finns behov av en möjlighet för regeringen att meddela sådana föreskrifter även fortsättningsvis. Visserligen torde vissa typer av föreskrifter som preciserar i vilka situationer personnummer eller samordningsnummer får behandlas av statliga myndigheter kunna meddelas av regeringen med stöd av 8 kap. 7 § 2 regeringsformen. Det kan dock inte uteslutas att det finns behov av föreskrifter som går utöver regeringens kompetens enligt nämnda lagrum, varför vi bedömer att ett bemyndigande behövs. Eftersom Datainspektionen hittills inte har sett anledning att utnyttja möjligheten enligt 16 § PUF att meddela föreskrifter och något behov av sådan vidaredelegation inte har framkommit, föreslår vi ingen sådan möjlighet.

En reglering av behandling av personnummer och samordningsnummer kan, oavsett om den tas in direkt i sektorsspecifik lag eller i förordning med stöd av bemyndigandet, tillåta behandling i andra fall än de som tillåts enligt den föreslagna bestämmelsen i dataskyddslagen. Detta förutsätter att regleringen i så fall lever upp till förordningens krav på lämpliga skyddsåtgärder för de registrerades fri- och rättigheter.

⁴ Se exempelvis prop. 2014/15:148 s. 51.

13 Begränsningar av vissa rättigheter och skyldigheter i dataskyddsförordningen

13.1 Vårt uppdrag

Dataskyddsförordningen ger medlemsstaterna möjlighet att begränsa omfattningen av vissa av de skyldigheter och rättigheter som förordningen föreskriver. Motsvarande reglering om möjligheten att föreskriva undantag finns i artikel 13.1 i dataskyddsdirektivet. Undantag med stöd av den bestämmelsen tas ofta in i sektorsspecifik lagstiftning. Det finns emellertid även i personuppgiftslagen ett generellt bemyndigande för regeringen att meddela föreskrifter om undantag av detta slag. Personuppgiftslagen innehåller vidare ett särskilt undantag från informationsskyldigheten vid sekretess och tystnadsplikt. I vårt uppdrag ingår att överväga om det finns behov av bestämmelser av detta slag i den generella regleringen som ska komplettera förordningen.

13.2 Dataskyddsförordningen

I artikel 23.1 anges att såväl unionsrätten som en medlemsstats nationella rätt får begränsa tillämpningsområdet för de skyldigheter och rättigheter som föreskrivs i artiklarna 12–22 och 34, samt artikel 5 i den mån dess bestämmelser motsvarar de rättigheter och skyldigheter som fastställs i artiklarna 12–22, om en sådan begränsning sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa vissa särskilt angivna mål, nämligen

- a) den nationella säkerheten,
- b) försvaret,
- c) den allmänna säkerheten,
- d) förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten,
- e) andra av unionens eller en medlemsstats viktiga mål av generellt allmänt intresse, särskilt ett av unionens eller en medlemsstats viktiga ekonomiska eller finansiella intressen, däribland penning-, budget- eller skattefrågor, folkhälsa och social trygghet,
- f) skydd av rättsväsendets oberoende och rättsliga åtgärder,
- g) förebyggande, förhindrande, utredning, avslöjande och lagföring av överträdelser av etiska regler som gäller för lagreglerade yrken,
- h) en tillsyns-, inspektions- eller regleringsfunktion som, även i enstaka fall, har samband med myndighetsutövning i fall som nämns i a–e och g,
- i) skydd av den registrerade eller andras rättigheter och friheter, och
- j) verkställighet av civilrättsliga krav.

I artikel 23.2 anges att sådana begränsningar ska innehålla specifika bestämmelser åtminstone, när så är relevant, avseende

- a) ändamålen med behandlingen eller kategorierna av behandling,
- b) kategorierna av personuppgifter,
- c) omfattningen av de införda begränsningarna,
- d) skyddsåtgärder för att förhindra missbruk eller olaglig tillgång eller överföring,
- e) specificeringen av den personuppgiftsansvarige eller kategorierna av personuppgiftsansvariga,

- f) lagringstiden samt tillämpliga skyddsåtgärder med beaktande av behandlingens art, omfattning och ändamål eller kategorierna av behandling,
- g) riskerna för de registrerades rättigheter och friheter, och
- h) de registrerades rätt att bli informerade om begränsningen, såvida detta inte kan inverka menligt på begränsningen.

13.3 Gällande rätt

I dataskyddsdirektivet finns motsvarigheten till förordningens artikel 23 i artikel 13.1. Bestämmelser i registerförfattningar som utgör undantag från de rättigheter och skyldigheter som föreskrivs i personuppgiftslagen har ofta sin grund i denna artikel. Det finns dock även några bestämmelser i personuppgiftslagen som har införts med stöd av artikel 13 i direktivet.

I 8 a § PUL finns ett generellt bemyndigande som anger att regeringen får meddela föreskrifter om undantag från 9, 23–26 och 28 §§ samt 29 § andra stycket och 42 §, om det är nödvändigt med hänsyn till de intressen som räknas upp i artikel 13.1 i dataskyddsdirektivet.

Enligt 26 § tredje stycket PUL behöver s.k. registerutdrag enligt första stycket samma paragraf inte lämnas om personuppgifter i löpande text som inte fått sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande. Undantaget gäller dock inte om uppgifterna har lämnats ut till tredje man eller om uppgifterna behandlas enbart för historiska, statistiska eller vetenskapliga ändamål eller, när det gäller löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats under längre tid än ett år. Bestämmelsen har införts med stöd av artikel 13.1 i direktivet, med hänsyn till skyddet av fri- och rättigheter.¹

I 27 § PUL anges att bestämmelserna i 23–26 §§ om den registrerades rätt till information inte gäller i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut till den registrerade. En personuppgiftsansvarig som inte är en myndighet får därvid i motsvarande fall som avses i offent-

¹ Prop. 1997/98:44 s. 81 f.

lighets- och sekretesslagen vägra att lämna ut uppgifter till den registrerade. Även denna bestämmelse har införts med stöd av artikel 13.1 i direktivet, med hänsyn till skyddet av fri- och rättigheter.²

13.4 Överväganden och förslag

Utredningens förslag: Skyldigheten att ge den registrerade information om och tillgång till de personuppgifter som behandlas ska inte gälla uppgifter som på grund av sekretess eller tystnadsplikt inte får lämnas ut till den registrerade.

Den registrerades rätt att på begäran få information om pågående personuppgiftsbehandling ska inte omfatta uppgifter som behandlas i löpande text som utgör utkast eller minnesanteckning. Undantaget ska dock inte gälla om uppgifterna har lämnats ut till tredje part, om uppgifterna behandlas enbart för arkivändamål av allmänt intresse eller för statistiska ändamål eller, när det gäller utkast, om uppgifterna har behandlats under mer än ett år.

Regeringen ska få meddela föreskrifter om ytterligare undantag från vissa av förordningens skyldigheter och rättigheter.

Utredningens bedömning: Rätten att göra invändningar bör inte inskränkas genom ett undantag i dataskyddslagen. Sådana undantag bör i stället övervägas på sektorspecifik nivå, om villkoren för behandling av personuppgifter specificeras genom författning.

13.4.1 Sekretess och tystnadsplikt ska gå före informationsplikten

Den personuppgiftsansvariges skyldighet att självmant tillhandahålla den registrerade information om behandlingen av personuppgifter framgår av 23–25 §§ PUL. Motsvarande bestämmelser finns i artiklarna 13 och 14 i dataskyddsförordningen. Den registrerade har vidare enligt 26 § första stycket PUL rätt att på begäran få information om och tillgång till de personuppgifter som behandlas. Motsvarande rätt, bland annat till s.k. registerutdrag, finns i artikel 15 i dataskyddsför-

² Prop. 1997/98:44 s. 83 f.

ordningen. Denna rätt ska enligt artikel 15.4 inte inverka menligt på andra rättigheter och friheter.

Personuppgiftslagens informationsskyldighet, och motsvarande rättighet för den registrerade, gäller enligt 27 § PUL inte om sekretess eller tystnadsplikt innebär att informationen inte ska lämnas ut till den registrerade. Frågan är om motsvarande undantag bör tas in i den generella lag som ska komplettera dataskyddsförordningen.

I artikel 14.5 föreskrivs flera direkt tillämpliga undantag från rätten till information, bland annat om personuppgifterna måste förbli konfidentiella till följd av tystnadsplikt enligt unionsrätt eller nationell rätt, inbegripet lagstadgade sekretessförpliktelser (led d). I artikel 15.4 anges endast att rätten till registerutdrag inte ska påverka menligt på andras friheter och rättigheter.

Det befintliga undantaget i 27 § PUL är något vidare än de direkt tillämpliga undantagen i artiklarna 14 och 15. Bestämmelsen i artikel 23 möjliggör dock ytterligare undantag på samma sätt som dataskyddsdirektivet. Det bör därför inte finnas något formellt hinder mot att en bestämmelse som motsvarar 27 § PUL tas in i dataskyddslagen.

Av det direkt tillämpliga undantaget i artikel 14.5 d i dataskyddsförordningen följer att den personuppgiftsansvarige inte på eget initiativ behöver förse den registrerade med information, om uppgifterna omfattas av sekretess eller tystnadsplikt. Det finns dock skäl att klargöra i dataskyddslagen att sekretess eller tystnadsplikt också kan medföra att en begäran om bekräftelse och information enligt artikel 15 ska avslås. Vidare finns det situationer då även en privaträttslig aktör, som inte omfattas av författningsreglerad sekretess eller tystnadsplikt, har berättigad anledning att hemlighålla uppgifter i förhållande till den registrerade. Det kan t.ex. röra sig om information som samlats in inför en domstolsprocess, om det kan antas att ett utlämnande av informationen skulle försämra den personuppgiftsansvariges ställning som part i rättegången.³

Dataskyddslagen bör därför förse med ett undantag från informationsplikten som i sak motsvarar 27 § PUL i dess helhet. Bestämmelsen respekterar enligt vår mening andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle. Förarbetsuttalanden

³ Prop. 1997/98:44 s. 83 f.

och praxis rörande 27 § PUL bör kunna vara vägledande även vid tillämpningen av den nya bestämmelsen.⁴

13.4.2 Löpande text som utgör utkast eller minnesanteckning ska inte omfattas av rätten till registerutdrag

Den registrerade har enligt 26 § första stycket PUL rätt att på begäran få information om och tillgång till de personuppgifter som behandlas. Bestämmelsen motsvarar artikel 12 a i dataskyddsdirektivet. Denna bestämmelse innebär dock enligt EU-domstolen inte en rätt att få del av den handling där personuppgifterna förekommer.⁵ Motsvarande rätt, bland annat till s.k. registerutdrag, finns i artikel 15 i dataskyddsförordningen. Denna rätt ska enligt artikel 15.4 inte inverka menligt på andra rättigheter och friheter.

Som nämns ovan anges i 26 § tredje stycket PUL att registerutdrag inte behöver lämnas om personuppgifter i löpande text som inte fått sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande. I förarbetena till detta undantag angavs, bland annat med hänvisning till regleringen i 2 kap. tryckfrihetsförordningen, att det på såväl den offentliga som den privata sidan finns goda skäl för en ordning som innebär att ofärdiga alster, minnesanteckningar och liknande inte behöver lämnas ut. Att under en rimlig tid få ha sina ofärdiga alster och minnesanteckningar i fred kunde enligt regeringens mening anses som en sådan fri- och rättighet som enligt artikel 13.1 i dataskyddsdirektivet berättigar till en begränsning av informationsskyldigheten. Men om uppgifterna behandlats under så lång tid som ett år utan att texten färdigställts, ansåg regeringen dock att den registrerades intresse av att få ta del av sina uppgifter skulle anses väga tyngre än den personuppgiftsansvariges intresse av att utan insyn få ytterligare fördröja färdigställandet av texten.⁶

Detta resonemang är enligt vår mening fortfarande relevant. Bestämmelsen respekterar enligt vår mening andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle. Mot den bak-

⁴ Se främst prop. 1997/98:44 s. 81 f.

⁵ Dom YS mot Minister voor Immigratie, C-141/12, EU:C:2014:2081, punkt 58.

⁶ Prop. 1997/98:44 s. 81 f.

grunden anser vi att det i den generella lagen bör tas in en bestämmelse som på motsvarande sätt som 26 § tredje stycket PUL gör undantag från rätten till information enligt artikel 15 i dataskyddsförordningen avseende personuppgifter i löpande text som inte fått sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande. Undantaget bör i likhet med gällande rätt inte gälla om uppgifterna har lämnats ut till tredje part eller om uppgifterna behandlas enbart för arkivändamål av allmänt intresse eller för statistiska ändamål eller, när det gäller löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats under längre tid än ett år. Frågan om huruvida undantaget ska gälla vid behandling för forskningsändamål bör däremot övervägas av Forskningsdatautredningen.

13.4.3 Något om rätten att göra invändningar

I artikel 21 i dataskyddsförordningen föreskrivs att den registrerade i vissa fall ska ha rätt att invända mot behandling av personuppgifter. Bestämmelsen är direkt tillämplig. En motsvarande rättighet föreskrivs även i dataskyddsdirektivet, men är genomförd i personuppgiftslagen endast såvitt avser direkt marknadsföring (11 § PUL). Dataskyddsförordningen innebär därmed att rätten att göra invändningar utvidgas jämfört med vad som följer av gällande svensk rätt.

Rätten att göra invändningar enligt artikel 21.1 i dataskyddsförordningen avser behandling av personuppgifter som grundar sig på artikel 6.1 e eller f. Rättigheten gäller alltså inte vid behandling av personuppgifter som exempelvis är nödvändig för att den personuppgiftsansvarige ska kunna uppfylla en rättslig förpliktelse (artikel 6.1 c), såsom när en myndighet genom författning ålagts att föra ett offentligt register. Följden av att en invändning görs enligt artikel 21.1 är att den personuppgiftsansvarige inte längre får behandla personuppgifterna, såvida inte denne kan påvisa tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk.

Enligt gällande svensk rätt har den registrerade inte någon generell rätt att göra invändningar mot den behandling av personuppgifter som sker hos myndigheter. Det finns mot den bakgrunden skäl att

särskilt överväga om dataskyddsförordningens rätt att göra invändningar bör inskränkas när det gäller sådan behandling som sker med stöd av artikel 6.1 e, dvs. med en fastställd uppgift av allmänt intresse som rättslig grund. Vi anser dock att denna rättighet fyller en viktig funktion ur rättssäkerhetssynpunkt, i synnerhet i de fall då de närmare villkoren för behandlingen inte har reglerats i en sektorsspecifik författning. Vi anser därför att rätten att göra invändningar mot myndigheters behandling av personuppgifter inte bör inskränkas på ett generellt plan genom ett undantag i dataskyddslagen. Sådana undantag bör i stället övervägas på sektorspecifik nivå, om villkoren för behandling av personuppgifter med stöd av artikel 6.1 e specificeras genom författning.

Jämfört med vad som gäller enligt personuppgiftslagen utgör det en nyhet också att den registrerade ges rätt att göra invändningar vid behandling som sker med stöd av artikel 6.1 f, dvs. med ett berättigat intresse som rättslig grund. Enligt vår mening skapar denna rättighet en bra balans mellan den personuppgiftsansvarige och den registrerade som inte bör rubbas genom ett generellt undantag. Vi lämnar därför inte något sådant förslag.

13.4.4 Regeringen ska få meddela föreskrifter om ytterligare undantag

Som redan har nämnts ger artikel 23 i dataskyddsförordningen, inom vissa angivna ramar, utrymme för att i sektorsspecifika författningar föreskriva undantag från förordningens bestämmelser. I den mån sådana undantag kan medföra ytterligare skyldigheter för enskilda eller kommuner eller innebära ingrepp i enskildas personliga förhållanden ska de enligt 8 kap. 2 § första stycket 2 och 3 regeringsformen föreskrivas genom lag. Den omständigheten att dataskyddslagen föreslås vara subsidiär till avvikande bestämmelser i lag eller förordning förändrar inte detta. Det krävs därför i vissa fall ett bemyndigande i lag för att sektorsspecifik särreglering i förordningsform även i fortsättningen ska kunna innehålla föreskrifter om undantag. Det bör därför införas ett bemyndigande i dataskyddslagen som i sak motsvarar det bemyndigande som finns i 8 a § PUL.

14 Arkiv och statistik

14.1 Vårt uppdrag

Enligt kommittédirektiven är det av central betydelse att myndigheternas bevarande av allmänna handlingar inte hindras av dataskyddsregleringen och att myndigheternas möjlighet att använda uppgifter i dessa handlingar säkerställs. Även behandling av personuppgifter för andra arkivändamål av allmänt intresse samt för vetenskapliga eller historiska forskningsändamål eller för statistiska ändamål måste garanteras. Samtidigt ska skyddet för den registrerades fri- och rättigheter beaktas. Utgångspunkten för vårt uppdrag är därför att vissa grundläggande bestämmelser, liknande de som i dag finns i personuppgiftslagen, behöver tas in i den generella reglering som ska komplettera dataskyddsförordningen.

Vi ska enligt direktiven analysera vilka bestämmelser om myndigheters bevarande av allmänna handlingar, användning av uppgifter i dessa och överlämnande av arkivmaterial till en arkivmyndighet som behövs i den generella regleringen. Vidare ska vi analysera vilka övriga bestämmelser om behandling av personuppgifter för arkivändamål av allmänt intresse samt för vetenskapliga eller historiska forskningsändamål eller för statistiska ändamål som bör finnas i den generella regleringen. Vi ska även lämna lämpliga författningsförslag.

Som framgår av avsnitt 2.2 har vi i samråd med Forschungsdatautredningen konstaterat att samtliga frågor rörande behandling av personuppgifter för forskningsändamål bör behandlas i ett samlat sammanhang och att Forschungsdatautredningen är bäst lämpad att göra den analys och de överväganden som krävs. Vi behandlar därför inte frågan om behandling av personuppgifter för forskningsändamål.

14.2 Gällande rätt

I personuppgiftslagen finns vissa centrala bestämmelser som rör lagens förhållande till myndigheters arkivering av allmänna handlingar och sådan personuppgiftsbehandling som sker för historiska, statistiska eller vetenskapliga ändamål.

Av 8 § andra stycket första meningen PUL framgår att lagens bestämmelser inte hindrar att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. I förarbetena till personuppgiftslagen bedömdes att myndigheternas bevarande av allmänna handlingar är tillåtet enligt de grundläggande bestämmelserna i dataskyddsdirektivet, så länge de inte innehåller känsliga personuppgifter. Ett särskilt undantag ansågs dock nödvändigt för att myndigheterna skulle kunna bevara också känsliga personuppgifter. Det aktuella undantaget i 8 § andra stycket första meningen PUL omfattar även den insamling och det långtidsbevarande av personuppgifter som sker hos de särskilda arkivmyndigheterna.¹

I 9 § PUL – där de grundläggande kraven på behandlingen av personuppgifter regleras – finns vissa bestämmelser som särskilt rör behandling för historiska, statistiska eller vetenskapliga ändamål. Här framgår exempelvis att en behandling av personuppgifter för sådana ändamål inte ska anses oförenlig med insamlingsändamålen (andra stycket). Det finns vidare regler om hur länge personuppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål (tredje stycket) och begränsningar av när personuppgifter som behandlas för sådana ändamål får användas för att vidta åtgärder i fråga om den registrerade (fjärde stycket). Sådana åtgärder får bara ske om den registrerade lämnat sitt samtycke eller det finns synnerliga skäl med hänsyn till den registrerades vitala intressen. Begränsningen har bedömts vara en sådan lämplig skyddsåtgärd som krävs enligt artikel 6 i dataskyddsdirektivet. Enligt 8 § andra stycket PUL gäller dock inte denna begränsning för myndigheters användning av personuppgifter i allmänna handlingar. Detta undantag bygger på att det för sådana personuppgifter finns andra lämpliga skyddsåtgärder i form av bestämmelser om sekretess och skydd för arkiv.²

¹ Prop. 1997/98:44 s. 47 f.

² Prop. 1997/98:44 s. 63.

Som tidigare har nämnts utgör bestämmelsen i 8 § andra stycket första meningen PUL ett undantag från förbudet mot att behandla känsliga personuppgifter. Känsliga personuppgifter får enligt 19 § första stycket PUL även behandlas för forskningsändamål, om behandlingen har godkänts enligt lagen om etikprövning av forskning som avser människor. I andra stycket samma paragraf anges att känsliga personuppgifter får behandlas också för statistikändamål, om behandlingen är nödvändig på sätt som sägs i 10 § och om samhällsintresset av det statistikprojekt där behandlingen ingår klart väger över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan innebära. Har behandlingen godkänts av en forskningsetisk kommitté, ska dessa förutsättningar enligt tredje stycket samma paragraf anses uppfyllda.

I 7 a § arkivförordningen (1991:446) föreskrivs undantag för arkivmyndigheten när det gäller den personuppgiftsansvariges skyldighet att lämna s.k. registerutdrag på begäran av den registrerade. I bestämmelsen anges att en arkivmyndighet inte behöver lämna besked och information enligt 26 § PUL när det gäller personuppgifter i arkivmaterial som tagits emot för förvaring av myndigheten, om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats. Avgränsningen till arkivmaterial som tagits emot för förvaring innebär att undantaget inte är tillämpligt på arkivmaterial som kommer från arkivmyndighetens egen verksamhet.

14.3 Dataskyddsförordningen

14.3.1 Direkt tillämpliga bestämmelser

I dataskyddsförordningen finns ett antal bestämmelser som särskilt rör personuppgiftsbehandling för arkivändamål av allmänt intresse samt för vetenskapliga eller historiska forskningsändamål eller för statistiska ändamål. Enligt artikel 5.1 b gäller exempelvis att ytterligare behandling (i det följande används den mer vedertagna termen vidarebehandling, om inte förordningstexten citeras) av personuppgifter för sådana ändamål, i enlighet med artikel 89.1, inte ska anses oförenlig med de ursprungliga ändamålen. Av artikel 5.1 e följer att personuppgifter får lagras under en längre tid än vad som normalt gäller, om uppgifterna enbart kommer att behandlas för arkivändamål i allmänhetens intresse eller för vetenskapliga eller historiska forsk-

ningsändamål eller för statistiska ändamål. Den förlängda bevarandetiden gäller i den mån som lämpliga tekniska och organisatoriska åtgärder vidtas i enlighet med kraven i artikel 89.1 för att säkerställa de registrerades fri- och rättigheter. Bestämmelserna i artikel 5 är direkt tillämpliga och kräver därmed inga nationella författningsåtgärder.

Bestämmelserna i artikel 14.1–4 om den personuppgiftsansvariges informationsplikt när personuppgifter inte har erhållits från den registrerade ska enligt artikel 14.5 b inte tillämpas i den mån tillhandahållandet av sådan information visar sig vara omöjligt eller skulle medföra en oproportionell ansträngning, särskilt vid behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1. I sådana fall ska den personuppgiftsansvarige vidta lämpliga åtgärder för att skydda den registrerades rättigheter och friheter och berättigade intressen, inbegripet göra uppgifterna tillgängliga för allmänheten. På motsvarande sätt anges i artikel 17.3 d att rätten till radering ("att bli bortglömd") inte gäller i den utsträckning som behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål enligt artikel 89.1, i den utsträckning som rätten att bli bortglömd sannolikt omöjliggör eller avsevärt försvårar uppnåendet av syftet med den behandlingen. Undantagen i artikel 14.5 b och 17.3 d är direkt tillämpliga.

Behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål ska enligt artikel 89.1 omfattas av lämpliga skyddsåtgärder för den registrerades rättigheter och friheter. Skyddsåtgärderna ska säkerställa att tekniska och organisatoriska åtgärder har införts för att se till att särskilt principen om uppgiftsminimering iakttas. Dessa åtgärder får inbegripa pseudonymisering, under förutsättning att ändamålen kan uppfyllas på det sättet. När ändamålen kan uppfyllas genom vidarebehandling av uppgifter som inte medger eller inte längre medger identifiering av de registrerade ska dessa ändamål uppfyllas på det sättet.

14.3.2 Bestämmelser som ger utrymme för nationella undantag

I artikel 9.1 i dataskyddsförordningen anges att behandling som avslöjar känsliga personuppgifter ska vara förbjuden, se avsnitt 10. Utrymmet för undantag från detta förbud, vid behandling som är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål, regleras i artikel 9.2 j. Där anges att förbudet inte gäller om behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenlig med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

Om personuppgifter behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål får det enligt artikel 89.2 i dataskyddsförordningen föreskrivas undantag från de rättigheter som avses i artiklarna 15, 16, 18 och 21, med förbehåll för de villkor och skyddsåtgärder som avses i artikel 89.1. Detta får emellertid bara göras i den utsträckning som sådana rättigheter sannolikt kommer att göra det omöjligt eller mycket svårare att uppfylla de särskilda ändamålen och sådana undantag krävs för att uppnå dessa ändamål. Möjligheten att föreskriva sådana undantag gäller enligt artikel 89.3 även avseende behandling av personuppgifter för arkivändamål av allmänt intresse. I detta fall får det dessutom föreskrivas undantag från de rättigheter som avses i artiklarna 19 och 20.

I artikel 15 regleras den registrerades rätt att få bekräftelse på om personuppgifter rörande honom eller henne behandlas och i så fall få viss information, bland annat ett s.k. registerutdrag (jfr 26 § PUL). Artikel 16 reglerar den registrerades rätt att få felaktiga personuppgifter rättade (jfr delar av 28 § PUL), medan artikel 18 ger den registrerade rätt att under vissa förutsättningar kräva att behandlingen begränsas. Om eventuella rättelser eller radering av personuppgifter eller begränsningar av behandling skett i enlighet med artiklarna 16, 17.1 och 18, ska den personuppgiftsansvarige enligt artikel 19 underrätta varje mottagare till vilken personuppgif-

terna har lämnats ut, om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning (jfr delar av 28 § PUL). Den personuppgiftsansvarige ska dessutom, på den registrerades begäran, informera denne om vilka dessa mottagare är.

Artikel 20, som saknar motsvarighet i personuppgiftslagen, reglerar rätten till dataportabilitet, dvs. den registrerades rätt att under vissa förutsättningar få ut sina personuppgifter i ett strukturerat, allmänt använt och maskinläsbart format och sedan överföra dessa till en annan personuppgiftsansvarig.

I artikel 21 i dataskyddsförordningen föreskrivs att den registrerade ska ha rätt att göra invändningar mot behandling av personuppgifter. Denna rätt gäller enligt artikel 21.1 bland annat vid behandling av personuppgifter som grundar sig på artikel 6.1 e eller f. Enligt artikel 21.6 får den registrerade motsätta sig behandling för vetenskapliga eller historiska forskningsändamål eller för statistiska ändamål av skäl som rör hans eller hennes personliga situation, om inte behandlingen är nödvändig för utförandet av en arbetsuppgift av allmänt intresse.

14.4 Överväganden och förslag – arkivändamål av allmänt intresse

14.4.1 Allmänt intresse

I dataskyddsförordningen används begreppet arkivändamål av allmänt intresse, i stället för det som i dataskyddsdirektivet benämns historiska ändamål. Begreppet allmänt intresse är ett unionsrättsligt begrepp som inte med enkelhet låter sig avgränsas. Begreppet definieras varken i dataskyddsdirektivet eller i dataskyddsförordningen och dess innebörd har ännu inte heller utvecklats av EU-domstolen. Rent språkligt kan begreppet allmänt intresse antas avse något som är av intresse för eller berör många människor på ett bredare plan, i motsats till ett särintresse. Den närmare innebörden av begreppet arkivändamål av allmänt intresse, särskilt i förhållande till begreppet historiska forskningsändamål, behöver dock klargöras i rättstillämpningen, inte minst genom EU-domstolens praxis.

Det står emellertid enligt vår mening klart att den behandling av personuppgifter som sker för att uppfylla krav på bevarande för andra syften, såsom exempelvis kravet på arkivering av räkenskaps-

information enligt bokföringslagen (1999:1078), inte utgör behandling för arkivändamål av allmänt intresse.

14.4.2 Rättslig grund och tillåten vidarebehandling

Utredningens förslag: Regeringen och Riksarkivet ska få meddela föreskrifter om behandling av personuppgifter för arkivändamål av allmänt intresse utanför arkivlagstiftningens tillämpningsområde. Riksarkivet ska även i förvaltningsbeslut få fastställa rättslig grund för ett enskilt organs behandling av personuppgifter för arkivändamål av allmänt intresse.

Utredningens bedömning: Myndigheter och andra organ som omfattas av arkivlagstiftningen har redan enligt gällande rättslig grund för behandling av personuppgifter för arkivändamål av allmänt intresse.

Vidarebehandling av personuppgifter för arkivändamål av allmänt intresse ska enligt dataskyddsförordningen inte anses vara oförenlig med de ursprungliga ändamålen. Någon rättslig grund behöver inte fastställas för sådan vidarebehandling.

Vad gäller för de organ som omfattas av arkivlagstiftningen?

Svenska myndigheter och vissa andra organ är enligt arkivlagen (1990:782) skyldiga att bevara sina allmänna handlingar. Myndigheternas arkiv är enligt 3 § arkivlagen en del av det nationella kulturarvet och ska bevaras, hållas ordnade och vårdas så att de tillgodoser rätten att ta del av allmänna handlingar, behovet av information för rättskipningen och förvaltningen samt forskningens behov. För tillsynen av att myndigheterna och andra organ fullgör sina skyldigheter enligt arkivlagen finns det arkivmyndigheter. Inom den statliga förvaltningen är Riksarkivet arkivmyndighet. En arkivmyndighet har enligt 9 § arkivlagen rätt att överta arkivmaterial från en myndighet som står under dess tillsyn, antingen efter överenskommelse eller på grund av ett ensidigt beslut från arkivmyndigheten.

Behandling av en viss personuppgift för andra ändamål än den ursprungligen samlades in är enligt artikel 5.1 b i dataskyddsförord-

ningen tillåten endast om vidarebehandlingen är förenlig med de ändamål som uppgiften ursprungligen samlades in för. I sådana fall, dvs. när vidarebehandlingen är förenlig med de ursprungliga ändamålen, krävs det enligt skäl 50 inte någon annan rättslig grund än den som gav legitimitet till att personuppgiften samlades in. Om behandlingen är nödvändig för att fullgöra en uppgift av allmänt intresse eller som ett led i myndighetsutövning som den personuppgiftsansvarige har i uppgift att utföra kan det enligt skäl 50 närmare föreskrivas för vilka uppgifter och syften ytterligare behandling bör anses som förenlig och laglig. Att ytterligare behandling för bland annat arkivändamål av allmänt intresse ska betraktas som förenlig och laglig behandling av uppgifter följer dock direkt av artikel 5.1 b.

Det står enligt vår mening klart att den behandling av personuppgifter som myndigheter och andra organ utför när de som en följd av arkivlagens bestämmelser arkiverar sina allmänna handlingar utgör en vidarebehandling som sker för arkivändamål av allmänt intresse. Behandlingen ska därmed enligt artikel 5.1 b inte anses som oförenlig med de ursprungliga ändamålen. Det krävs då inte någon annan separat rättslig grund än den med stöd av vilken insamlingen av personuppgifter medgavs (skäl 50).

Vidarebehandling är det bara fråga om när ett och samma organ, eller dennes personuppgiftsbiträde, utför ytterligare behandlingar avseende en viss uppgift. När en arkivmyndighet, t.ex. Riksarkivet, övertar arkivmaterial från en annan myndighet övergår hela ansvaret för det materialet till arkivmyndigheten (9 § tredje stycket arkivlagen). Den myndighet som har överlämnat materialet förfogar därefter inte längre över detta. Den myndigheten bestämmer inte heller längre över ändamålen och medlen för arkivmyndighetens behandling av de personuppgifter som förekommer i materialet. I dataskyddsförordningens mening kan arkivmyndigheten därför inte betraktas som ett personuppgiftsbiträde, som endast vidarebehandlar uppgifter för den andra myndighetens räkning. Arkivmyndigheten bär i stället personuppgiftsansvaret för de behandlingar som sker därefter (se definitionen av begreppet personuppgiftsansvarig i artikel 4.7 i dataskyddsförordningen). En arkivmyndighet är givetvis även, precis som alla andra myndigheter, personuppgiftsansvarig för all annan behandling av personuppgifter som utförs i den egna verksamheten.

Detta innebär att det behövs en rättslig grund för arkivmyndigheternas insamling och annan behandling av de personuppgifter som

finns i det material som övertas från andra myndigheter. Den behandlingen sker för att utföra en i arkivlagstiftningen fastställd uppgift av allmänt intresse (se avsnitt 8.3.4). Nödvändig behandling hos arkivmyndigheterna kan därmed ske med dessa bestämmelser som rättslig grund, enligt artikel 6.1 e i dataskyddsförordningen.

Vad gäller för enskilda arkiv?

Organ som inte omfattas av arkivlagstiftningen kan i vissa fall också ha anledning att behandla personuppgifter för arkivändamål av allmänt intresse. Om syftet med behandlingen är just detta, och inte t.ex. historiska forskningsändamål, måste dock bedömas från fall till fall. Av skäl 158 till dataskyddsförordningen framgår att ett sådant organ bör ha en rättslig skyldighet att förvärva, bevara, bedöma, organisera, beskriva, kommunicera, främja, sprida och ge tillgång till uppgifter av bestående värde för allmänintresset. Medlemsstaterna bör enligt samma skäl också ha rätt att föreskriva att personuppgifter får vidarebehandlas för arkivering, exempelvis i syfte att tillhandahålla specifik information om politiskt beteende under tidigare totalitära regimer, folkmord, brott mot mänskligheten, särskilt Förintelsen, eller krigsförbrytelser.

Det bör noteras att dataskyddsförordningen inte gäller för behandling av personuppgifter som avser avlidna personer (skäl 27). Detta innebär i praktiken att många enskilda arkiv inte berörs av dataskyddsregleringen, såsom historiska släktarkiv eller liknande samlingar som inte innehåller några uppgifter om nu levande personer.

Insamling av arkivmaterial som innehåller personuppgifter

Det finns i Sverige ett antal enskilda arkivinstitutioner, såväl regionala som nationella, som samlar in personuppgifter enbart för arkivändamål av allmänt intresse. Den rättsliga grunden för denna behandling torde i normalfallet vara att verksamheten är av allmänt intresse. Det är dock oklart om denna uppgift alltid är fastställd i enlighet med svensk rätt. När dataskyddsförordningen börjar tillämpas kan därmed den rättsliga grunden för de enskilda arkivinstitutionernas behandling av personuppgifter komma att ifrågasättas. Det bör därför införas en bestämmelse i dataskyddslagen som gör det möjligt för regeringen

eller den myndighet som regeringen bestämmer att meddela föreskrifter som tillåter behandling av personuppgifter för arkivändamål av allmänt intresse också utanför arkivlagstiftningens tillämpningsområde. Föreskriftsrätten bör enligt vår mening delegeras till Riksarkivet.

Det är tänkbart att det kan uppstå enstaka situationer där föreskriftsformen inte är lämplig, men där det ändå finns skäl att tillåta behandling för arkivändamål av allmänt intresse. Det kan till exempel röra sig om behandling som ska ske av ett enskilt organ under en begränsad tid eller i ett mycket begränsat avseende. I likhet med den ordning som gäller avseende behandling av personuppgifter om lagöverträdelse enligt 21 § PUL, och som föreslås i avsnitt 11.4, bör därför Riksarkivet i enskilda fall kunna pröva om den behandling som sker hos en enskild aktör är arkivverksamhet av allmänt intresse i dataskyddsförordningens mening. De närmare kriterierna för denna prövning skulle vid behov kunna fastställas i föreskrifter på lägre normnivå. Om arkivverksamheten uppfyller dataskyddsförordningens krav kan det enskilda organet genom ett särskilt beslut medges rätt att behandla personuppgifter för arkivändamål av allmänt intresse. Den personuppgiftsbehandling som är nödvändig för detta ändamål kan då ske med beslutet som rättslig grund. Ett förvaltningsbeslut som går organet emot bör kunna överklagas, se avsnitt 19.8.

Det bör noteras att regeringen, i propositionen om kulturarvs politik, har bedömt att det finns anledning att genomföra en bred översyn av arkivväsendet i landet och att denna översyn även ska tydliggöra de enskilda arkivens viktiga roll som en del av det gemensamma kulturarvet.³ Vi välkomnar en sådan översyn och förutsätter att frågor kring de enskilda arkivens behandling av personuppgifter då kommer att utredas närmare.

³ Prop. 2016/17:116, s. 174 f.

Vidarebehandling av personuppgifter

Det förekommer att enskilda organ har skäl att bevara uppgifter under en längre tid än vad som krävs för det ursprungliga ändamålet. En sådan vidarebehandling skulle bland annat kunna ske för arkivändamål av allmänt intresse eller för historiska forskningsändamål. Behandling av personuppgifter för forskningsändamål omfattas emellertid inte av våra överväganden, utan tas om hand av Forskningsdatautredningen.

Vidarebehandling av personuppgifter för arkivändamål av allmänt intresse ska enligt artikel 5.1 b inte anses som oförenlig med de ursprungliga ändamålen. Det krävs därmed i och för sig inte någon annan separat rättslig grund än den med stöd av vilken insamlingen av personuppgifter medgavs (skäl 50). Det kan dock i det enskilda fallet vara svårt för den personuppgiftsansvarige, den registrerade och tillsynsmyndigheten att bedöma om arkivverksamheten är av allmänt intresse på det sätt som avses i dataskyddsförordningen. I de fall detta inte följer direkt av de föreskrifter som har meddelats bör den personuppgiftsansvarige ha samma möjlighet som enskilda arkivinstitutioner att få frågan prövad och fastställd genom förvaltningsbeslut.

Enskilda arkiv som överlämnas till Riksarkivet

Enskilda arkiv som överlämnas till Riksarkivet för förvaring utgör en kategori som bör beröras särskilt. Enligt 6 § andra stycket förordningen (2009:1593) med instruktion för Riksarkivet får Riksarkivet ta emot arkivhandlingar från enskilda om de är av särskild betydelse för forskning och kulturarv. Enligt vår bedömning innebär detta att sådana arkiv måste anses vara av allmänt intresse. Handlingar som har tagits emot för förvaring ska dessutom enligt 7 § samma förordning hållas tillgängliga. Som exempel på enskilda arkiv som överlämnats till Riksarkivet på denna grund kan nämnas de s.k. idrottsarkiven, som härrör från bland annat Riksidrottsförbundets verksamhet.

Den vidarebehandling som utförs för att bilda denna typ av enskilda arkiv ska enligt artikel 5.1 b i dataskyddsförordningen, på grund av att den sker för arkivändamål av allmänt intresse, anses vara förenlig med det ändamål för vilket uppgifterna ursprungligen samlades in. Den insamling av personuppgifter som Riksarkivet utför i samband med att en sådant enskilt arkiv lämnas in sker med stöd av myn-

dighetens instruktion och utgör därmed en fastställd uppgift av allmänt intresse. Riksarkivets behandling av de personuppgifter som finns i de enskilda arkiven kan därmed ske på denna rättsliga grund, enligt artikel 6.1 e i dataskyddsförordningen.

Det förekommer också att enskilda arkiv överlämnas till Riksarkivet som deposition, dvs. utan att äganderätten övergår. I sådana fall kan parterna avtala om att Riksarkivet ska ges ett privaträttsligt uppdrag att i egenskap av personuppgiftsbiträde förvara och vårda materialet för deponentens räkning.

14.4.3 Förhållandet till arkivlagstiftningen och behandling av känsliga personuppgifter

Utredningens förslag: Känsliga personuppgifter och uppgifter om lagöverträdelser ska få behandlas om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om bevarande och vård av arkiv.

Regeringen och Riksarkivet ska få meddela föreskrifter som också i andra fall tillåter behandling av känsliga personuppgifter för arkivändamål av allmänt intresse. Riksarkivet ska även i enskilda fall få besluta att ett enskilt organ får behandla sådana personuppgifter för arkivändamål av allmänt intresse.

Bestämmelsen i 8 § andra stycket första meningen PUL tydliggör att personuppgiftslagen inte hindrar att en myndighet, i enlighet med arkivbestämmelserna, arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. I praktiken innebär detta att arkivlagstiftningen har företräde framför personuppgiftslagen. Detta är en nödvändig utgångspunkt för att den svenska offentlighetsprincipen fullt ut ska kunna fylla sin funktion. Det finns ingenting i dataskyddsförordningen som förhindrar att ett sådant synsätt bibehålls. Tvärtom säkerställs offentlighetsprincipens ställning genom artikel 86 i förordningen.

Lagring och annan behandling av personuppgifter för arkivändamål av allmänt intresse är dessutom särskilt gynnad i dataskyddsförordningen, precis som i dataskyddsdirektivet. Det är till exempel tillåtet att bevara personuppgifter under längre tid än vad som annars är nödvändigt, i den mån uppgifterna enbart behandlas för arkivända-

mål av allmänt intresse och under förutsättning att lämpliga tekniska och organisatoriska åtgärder genomförs (artiklarna 5.1 e och 89.1).

Vad gäller behandling av känsliga personuppgifter ger artikel 9.2 j i dataskyddsförordningen ett tydligare utrymme för undantag än dataskyddsdirektivet. I bestämmelsen anges att behandling får ske för arkivändamål av allmänt intresse, på grundval av unionsrätten eller nationell rätt som står i proportion till det eftersträvade syftet, är förenlig med det väsentliga innehållet i rätten till dataskydd och innehåller bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades rättigheter och intressen.

Behandling för arkivändamål av allmänt intresse av personuppgifter som inte utgör känsliga personuppgifter regleras av direkt tillämpliga bestämmelser i dataskyddsförordningen. Vidare följer det direkt av förordningen att vidarebehandling av personuppgifter för arkivändamål av allmänt intresse inte ska anses som oförenlig med de ursprungliga ändamålen. Det behövs därmed, enligt skäl 50, inte någon separat rättslig grund för en sådan behandling. Det faktum att behandling av känsliga personuppgifter för arkivändamål särbehandlas i artikel 9.2 j i dataskyddsförordningen talar dock för att all behandling av känsliga personuppgifter för arkivändamål, även vidarebehandling, måste omfattas av en särskild undantagsreglering för att vara tillåten. Denna bestämmelse förutsätter nämligen att gällande rätt innehåller bestämmelser om lämpliga och särskilda skyddsåtgärder för att säkerställa den registrerades rättigheter och intressen. Den vidarebehandling av känsliga personuppgifter som myndigheter och andra organ utför som en följd av arkivlagens bestämmelser är därmed inte tillåten enbart på grundval av det undantag från förbudet som tillämpats vid behandlingen för det ursprungliga ändamålet.

Vi bedömer därför att det i dataskyddslagen behövs en bestämmelse som i likhet med 8 § andra stycket första meningen PUL tillåter att en myndighet arkiverar och bevarar allmänna handlingar som innehåller känsliga personuppgifter samt att arkivmaterial som innehåller känsliga personuppgifter tas om hand av en arkivmyndighet. Den svenska lagstiftningen på detta område, med beaktande av de skyddsåtgärder som föreskrivs i form av sekretess och i registerförfattningar och genom gallringsföreskrifter, måste i sig anses vara proportionell till det eftersträvade syftet och förenlig med det väsentliga innehållet i rätten till dataskydd.

Eftersom behandling för arkivändamål av allmänt intresse av personuppgifter som inte utgör känsliga personuppgifter regleras av direkt tillämpliga bestämmelser i dataskyddsförordningen bör bestämmelsen i dataskyddslagen utformas som ett undantag från förbudet mot behandling av känsliga personuppgifter. Vi föreslår således att dataskyddslagen ska innehålla en bestämmelse som anger att känsliga personuppgifter får behandlas om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om bevarande och vård av arkiv. Bestämmelsen medför att dataskyddsförordningen och dataskyddslagen inte hindrar att allmänna handlingar arkiveras och bevaras eller att arkivmaterial tas om hand av en arkivmyndighet. Den författningstekniska skillnaden mellan 8 § andra stycket första meningen PUL och den bestämmelse som vi föreslår innebär således ingen saklig förändring i denna del.

Arkivlagstiftningen omfattar inte bara myndigheter utan även vissa utpekade enskilda organ. För dessa organ skulle det i enstaka fall kunna uppstå en normkonflikt mellan arkivlagstiftningen och begränsningen i artikel 10 i dataskyddsförordningen avseende enskildas behandling av personuppgifter om lagöverträdelse (se kapitel 11). Dataskyddslagen bör därför även innehålla en bestämmelse som, på motsvarande sätt som avseende känsliga personuppgifter, tillåter behandling av personuppgifter om lagöverträdelse, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om bevarande och vård av arkiv.

När det gäller enskilda arkiv som inte omfattas av arkivlagstiftningen finns det inga föreskrifter om bevarande och vård av arkiv som ska följas. Det kan dock även hos dessa organ finnas ett allmänt intresse av att känsliga personuppgifter bevaras. Sådant bevarande bör enligt vår bedömning också tillåtas under vissa förutsättningar. Risken är annars uppenbar att viktig information om vår samtid för alltid går förlorad. Det bör därför införas en bestämmelse i dataskyddslagen som anger att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter som tillåter att känsliga personuppgifter får behandlas för arkivändamål av allmänt intresse. Föreskriftsrätten bör delegeras till Riksarkivet. Riksarkivet bör även i enskilda fall få besluta att ett enskilt organ får behandla sådana personuppgifter för arkivändamål av allmänt intresse. Ett sådant förvaltningsbeslut bör lämpligen meddelas i samband med att den rättsliga grunden fastställs för organets behandling av personuppgifter för

arkivändamål av allmänt intresse. Beslutet kan även meddelas som komplement till en tidigare antagen föreskrift som ger organet rättslig grund för behandling av personuppgifter för detta ändamål.

För enskilda arkiv finns det inte några generella föreskrifter om särskilda skyddsåtgärder, utöver dem som följer direkt av dataskyddsförordningen och den som vi föreslår i följande avsnitt. Mot bakgrund av att de enskilda arkiven sinsemellan uppvisar stora olikheter är det heller inte lämpligt att i lag slå fast att en viss typ av ytterligare skyddsåtgärd alltid ska gälla vid behandling av känsliga personuppgifter. Det bör i stället ankomma på regeringen eller Riksarkivet att bedöma om beslut som tillåter ett enskilt organ att behandla känsliga personuppgifter och personuppgifter om lagöverträdelse ska villkoras av att den personuppgiftsansvarige vidtar särskilda åtgärder och i så fall vilka. Vidare följer det givetvis direkt av dataskyddsförordningen att ett beslut som tillåter behandling av känsliga personuppgifter bara kan tillämpas om behandlingen i sig vilar på rättslig grund eller utgör en tillåten vidarebehandling.

14.4.4 Lämpliga skyddsåtgärder

Utredningens förslag: Personuppgifter som behandlas enbart för arkivändamål av allmänt intresse ska inte få användas för att vidta åtgärder i fråga om den registrerade annat än om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen. Denna begränsning ska inte hindra en myndighet från att använda personuppgifter som finns i allmänna handlingar.

Behandling av personuppgifter för arkivändamål av allmänt intresse ska enligt artikel 89.1 i dataskyddsförordningen omfattas av lämpliga skyddsåtgärder för den registrerades rättigheter och friheter. Denna bestämmelse, som är direkt tillämplig, är den personuppgiftsansvarige skyldig att följa. För att behandling av känsliga personuppgifter ska vara tillåten för arkivändamål av allmänt intresse krävs dessutom, enligt artikel 9.2 j, att unionsrätten eller den nationella rätten innehåller bestämmelser om sådana åtgärder.

I 9 § fjärde stycket PUL anges, som en generell skyddsåtgärd, att personuppgifter som behandlas för historiska, statistiska eller vetenskapliga ändamål får användas för att vidta åtgärder i fråga om den

registrerade bara om den registrerade har lämnat sitt samtycke eller det finns synnerliga skäl med hänsyn till den registrerades vitala intressen. Enligt 8 § andra stycket PUL gäller dock denna begränsning inte för en myndighets användning av personuppgifter i allmänna handlingar.

När en personuppgift inte längre behöver behandlas för det ursprungliga ändamålet ska den, enligt huvudregeln i artikel 5.1 e i dataskyddsförordningen, gallras eller anonymiseras. Undantag gäller dock om det finns ett berättigat arkivändamål av allmänt intresse. Möjligheten till förlängd bevarandetid förutsätter att uppgiften ”enbart” behandlas för arkivändamål. Det kan emellertid inte uteslutas att en arkiverad uppgift åter kan komma att behövas även för andra ändamål, t.ex. i den personuppgiftsansvariges kärnverksamhet. Begränsningen i 9 § fjärde stycket PUL förhindrar sådan återanvändning i vissa situationer. Frågan är om en motsvarande skyddsåtgärd bör införas även i dataskyddslagen. För att kunna ta ställning till denna fråga är det nödvändigt att först analysera innebörden av den s.k. finalitetsprincipen.

Finalitetsprincipen

Dataskyddsförordningen bygger, precis som dataskyddsdirektivet och personuppgiftslagen, på förutsättningen att varje ny behandling ska prövas mot det ändamål för vilket uppgifterna ursprungligen samlades in av den personuppgiftsansvarige. I artikel 5.1 b i förordningen anges nämligen att uppgifter inte får behandlas på ett sätt som är oförenligt med de ändamål för vilka uppgifterna samlades in. Bestämelsen ger uttryck för den s.k. finalitetsprincipen. Denna begränsning är relevant i förhållande till varje behandling som den personuppgiftsansvarige eller dennes biträde utför efter själva insamlingen. Varje efterföljande behandlingsåtgärd, inklusive den tekniska bearbetning och lagring som ofta är oundviklig när uppgifter har samlats in, utgör nämligen en ytterligare behandling (dvs. vidarebehandling) i förordningens mening. Detta gäller enligt artikel 29-gruppen oavsett om denna behandling sker för samma ändamål som det för vilka uppgifterna samlades in eller för något annat ändamål.⁴

⁴ Jfr Artikel 29-gruppens yttrande 3/2013 om ändamålsbegränsning, s. 21.

En uppgift som bevaras hos en personuppgiftsansvarig endast för arkivändamål av allmänt intresse, t.ex. som en följd av arkivlagstiftningen, har normalt inte samlats in för just detta ändamål (utom hos Riksarkivet och andra arkivmyndigheter). Uppgiften har i stället samlats in för något helt annat ändamål, såsom för handläggning av ett ärende i den personuppgiftsansvariges kärnverksamhet. Arkiveringen utgör därför en vidarebehandling, som är tillåten eftersom den inte ska anses oförenlig med det ursprungliga ändamål för vilket uppgiften samlades in. Det är viktigt att notera att det är i förhållande till detta ursprungliga insamlingsändamål som varje vidarebehandling även av en arkiverad uppgift ska prövas. Finalitetsprincipen innebär nämligen inte att behandlingen ska prövas mot det ändamål för vilket den senaste vidarebehandlingen utfördes, i detta fall arkivändamålet. Dataskyddsförordningen, liksom dataskyddsdirektivet, förbjuder endast vidarebehandling som är oförenlig med det ursprungliga insamlingsändamålet. Detta innebär att vidarebehandling kan ske för nya ändamål som är oförenliga med varandra, så länge de nya ändamålen var för sig inte är oförenliga med det ursprungliga insamlingsändamålet.

Finalitetsprincipen utgör således inte i sig något hinder mot att en uppgift som har bevarats hos den personuppgiftsansvarige enbart för arkivändamål återförs till kärnverksamheten för vidarebehandling, förutsatt att den nya behandlingen är förenlig med det ursprungliga insamlingsändamålet. I en sådan situation behöver den personuppgiftsansvarige varken samla in uppgiften på nytt eller inhämta den registrerades samtycke till behandlingen. Den nya behandlingen kräver enligt dataskyddsförordningen inte heller någon annan rättslig grund än den med stöd av vilken den ursprungliga insamlingen medgavs (skäl 50). Det är alltså endast förenligheten med insamlingsändamålet som måste bedömas. Detta skiljer sig från det synsätt som har gällt hittills, nämligen att varje vidarebehandling måste kunna hänföras till något av de tillåtna fall av behandling som anges i 10 § PUL.

En arkiverad uppgift kan lika lite som någon annan uppgift behandlas för ett ändamål som är oförenligt med det ursprungliga insamlingsändamålet. Uppgiften måste i ett sådant fall samlas in på nytt, trots att den faktiskt redan finns hos den personuppgiftsansvarige. I vissa fall kan det dock vara tillräckligt att hämta in den registrerades samtycke till att den arkiverade uppgiften behandlas för nya

ändamål.⁵ Ett sådant nytt samtycke utgör då rättslig grund för den nya behandlingen.

Bör dataskyddslagen innehålla en användningsbegränsning?

Enligt 9 § fjärde stycket PUL, läst tillsammans med 8 § andra stycket andra meningen PUL, får inga andra än myndigheter använda arkiverade personuppgifter för att vidta en åtgärd i fråga om den registrerade, om inte den registrerade själv har lämnat sitt samtycke eller det finns synnerliga skäl med hänsyn till den registrerades vitala intressen. Bestämmelsen utgör därmed en begränsning av möjligheten att behandla arkiverade uppgifter för andra ändamål än arkivändamålet. Denna begränsning gäller oavsett om den nya behandlingen skulle ske för det ursprungliga insamlingsändamålet eller för något annat därmed förenligt ändamål. Av förarbetena framgår dock att bestämmelsen inte aktualiseras om en arkiverad uppgift även behandlas för andra ändamål, dvs. inte enbart för arkivändamål.⁶ En uppgift som fortfarande behövs i kärnverksamheten och därför behandlas där kan alltså användas för att vidta åtgärder i fråga om den registrerade, även om samma uppgift också förekommer i en arkiverad handling hos den personuppgiftsansvarige.

Förarbetena till 9 § fjärde stycket PUL ger ingen vägledning rörande vad som avses med uttrycket ”åtgärder i fråga om den registrerade”. I doktrinen har dock framförts att enbart ett utlämnande av personuppgifterna till tredje man inte torde innebära att en åtgärd vidtas i fråga om den registrerade, ens om tredje man avser att vidta en sådan åtgärd.⁷

Som exempel på när det skulle kunna finnas synnerliga skäl med hänsyn till den registrerades vitala intressen nämns i förarbetena att en forskare som har upptäckt ett samband mellan en medicin och en allvarlig sjukdom måste kunna använda arkiverade personuppgifter för att varna dem som tagit medicinen.⁸

⁵ Artikel 29-gruppens yttrande 3/2013 om ändamålsbegränsning, s. 26.

⁶ SOU 1997:39 s. 359 f.

⁷ Öman och Lindblom, Personuppgiftslagen (20 december 2016, Zetco), kommentaren till 9 § fjärde stycket PUL.

⁸ Prop. 1997:98:44 s. 120.

Enligt vår bedömning utgör bestämmelsen i 9 § fjärde stycket PUL en väl avvägd skyddsåtgärd. En motsvarande begränsning bör därför införas även i dataskyddslagen och bör, precis som den nu gällande bestämmelsen, inte bara avse känsliga personuppgifter. Den nya bestämmelsen bör dock utformas så att det tydligare än i dag framgår att användningsbegränsningen bara gäller personuppgifter som *enbart* behandlas för arkivändamål av allmänt intresse. Det finns vidare inget skäl att ange i paragrafen att uppgifter får användas med den registrerades samtycke. Om samtycke inhämtas till att en arkiverad uppgift används för nya ändamål, kan behandlingen nämligen jämföras med personuppgiften samlas in på nytt med stöd av artikel 6.1 a i data-skyddsförordningen.⁹ Någon saklig skillnad mellan vårt förslag och 9 § fjärde stycket PUL är inte avsedd.

Vad gäller myndigheternas arkiv utgör de nationella författningsbestämmelserna om sekretess en särskild skyddsåtgärd, eftersom dessa har utformats noggrant efter en avvägning mellan behovet av skydd och intresset av insyn. Dessutom omfattas myndigheternas arkiv av allmänna bestämmelser om skydd av arkiv, bland annat Riksarkivets föreskrifter, och krav på avskiljande i registerförfattningar. Ytterligare skyddsåtgärder, t.ex. i form av användningsbegränsningar som förhindrar återanvändning av arkiverade uppgifter, bör vid behov införas i sektorsspecifika författningar och inte i den generella lagen. Den föreslagna bestämmelsen om begränsningar av möjligheten att vidta åtgärder i fråga om den registrerade ska därför inte hindra myndigheter från att använda personuppgifter som finns i allmänna handlingar. Förslaget medför därmed ingen förändring i förhållande till vad som gäller enligt personuppgiftslagen.

⁹ Jfr Artikel 29-gruppens yttrande 3/2013 om ändamålsbegränsning, s. 27.

14.4.5 Undantag från vissa av den registrerades rättigheter

Utredningens förslag: Hänvisningen till personuppgiftslagen i arkivförordningens bestämmelse om undantag från rätten till s.k. registerutdrag ska ersättas med en hänvisning till dataskyddsförordningen.

En arkivmyndighet ska inte behöva rätta, komplettera eller begränsa behandlingen av personuppgifter i arkivmaterial som tagits emot för förvaring av myndigheten.

Rätten att göra invändningar ska inte gälla vid arkivmyndigheters behandling av personuppgifter i arkivmaterial som tagits emot för förvaring av myndigheten.

Om personuppgifter behandlas för arkivändamål av allmänt intresse får det enligt artikel 89.3 i dataskyddsförordningen föreskrivas undantag från de rättigheter som avses i artiklarna 15, 16, 18, 19, 20 och 21, med förbehåll för de villkor och skyddsåtgärder som avses i artikel 89.1 (se avsnitt 14.3.2). Detta får emellertid bara göras i den utsträckning som sådana rättigheter sannolikt kommer att göra det omöjligt eller mycket svårare att uppfylla de särskilda ändamålen och sådana undantag krävs för att uppnå detta ändamål.

Såväl offentliga som enskilda arkiv fyller en viktig samhällsfunktion. I synnerhet är väl fungerande myndighetsarkiv av grundläggande betydelse för forskning och utveckling, insyn och delaktighet, ansvarsutkrävande och demokrati. Detta intresse kan i vissa situationer väga tyngre än den enskildes intresse av att kunna utöva sina rättigheter enligt dataskyddsförordningen. Det finns därför skäl att överväga om Sverige bör utnyttja det utrymme som förordningen ger för att föreskriva undantag från vissa av dessa rättigheter, om det annars skulle bli omöjligt eller mycket svårare att uppfylla arkivändamålet. Vår allmänna utgångspunkt är dock att de registrerades rättigheter inte bör inskränkas i större utsträckning än vad som gäller enligt gällande rätt.

Rätten till tillgång (s.k. registerutdrag)

Motsvarigheten till artikel 15 i dataskyddsförordningen, rörande den registrerades rätt att på begäran få besked om huruvida personuppgifter som rör honom eller henne behandlas (s.k. registerutdrag), finns i 26 § PUL. I tredje stycket i denna paragraf anges att sådan information inte behöver lämnas om personuppgifter i löpande text som inte fått sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande. Detta undantag gäller dock inte om uppgifterna har lämnats ut till tredje man eller om uppgifterna behandlas enbart för historiska, statistiska eller vetenskapliga ändamål eller, när det gäller löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats under längre tid än ett år.

Undantaget i 26 § tredje stycket PUL är därmed inte tillämpligt vid sådan behandling som sker för arkivändamål av allmänt intresse. Den registrerades rätt till registerutdrag enligt personuppgiftslagen omfattar således alla typer av arkiverade uppgifter, även i form av minnesanteckningar eller liknande. Denna ordning bör enligt vår bedömning bestå. Vi ser således inte skäl att föreslå något generellt undantag från rätten till information enligt artikel 15 i dataskyddsförordningen vid behandling av personuppgifter för arkivändamål av allmänt intresse. Frågan om behovet i övrigt av undantag från rätten till registerutdrag behandlas i avsnitt 13.

I 7 a § arkivförordningen anges emellertid att en arkivmyndighet inte behöver lämna besked och information enligt 26 § PUL när det gäller personuppgifter i arkivmaterial som tagits emot för förvaring av myndigheten, om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats. Vi anser att ett liknande undantag från artikel 15 i dataskyddsförordningen krävs för att arkivändamålet för behandling av personuppgifter i Riksarkivets och andra arkivmyndigheters verksamhet även i fortsättningen ska kunna uppnås. Vi föreslår därför att 7 a § arkivförordningen ändras på så sätt att hänvisningen till 26 § PUL byts ut mot artikel 15 i dataskyddsförordningen. Det bör noteras att undantaget kan tillämpas endast under förutsättning att de direkt tillämpliga villkoren i artikel 89.1 i dataskyddsförordningen om bland annat skyddsåtgärder och uppgiftsminimering efterlevs.

Rätten till rättelse av personuppgifter och begränsning av behandling

Enligt artikel 16 i dataskyddsförordningen har den registrerade rätt att få felaktiga personuppgifter rättade och ofullständiga personuppgifter kompletterade. Artikel 18 ger den registrerade rätt att under vissa omständigheter kräva att behandlingen av personuppgifter begränsas. Bestämmelsernas motsvarighet finns i 28 § PUL första meningen, som anger att den personuppgiftsansvarige är skyldig att på begäran av den registrerade snarast bland annat rätta eller blockera sådana personuppgifter som inte har behandlats i enlighet med personuppgiftslagen eller föreskrifter som har utfärdats med stöd av den lagen. Personuppgiftslagen innehåller inte något undantag från dessa rättigheter och det gör inte heller arkivlagstiftningen. Vi anser att det inte heller i förhållande till artiklarna 16 och 18 i dataskyddsförordningen bör införas något generellt undantag från den registrerades rättigheter vid behandling av personuppgifter för arkivändamål av allmänt intresse.

Riksarkivet och andra arkivmyndigheter utför inte några rättelser i de handlingar som bevaras där, bland annat eftersom det skulle utgöra en otillåten förvanskning av allmänna handlingar. En rättelse kan i det enskilda fallet även riskera att försämra den enskildes rättigheter, om den medför att det inte längre är möjligt att i efterhand kontrollera myndigheternas verksamhet och ge upprättelse om ett fel har begåtts. Riksarkivet blockerar inte heller personuppgifter i arkiven. Enligt vår bedömning krävs det ett uttryckligt undantag från artiklarna 16 och 18 i dataskyddsförordningen för att denna etablerade hantering ska kunna fortgå, vilket i sin tur är en förutsättning för att offentlighetsprincipen ska kunna upprätthållas.

Det bör därför införas en bestämmelse i arkivförordningen som anger att en arkivmyndighet inte behöver rätta eller komplettera personuppgifter enligt artikel 16 i dataskyddsförordningen, när det gäller personuppgifter i arkivmaterial som tagits emot för förvaring av myndigheten. På motsvarande sätt bör arkivmyndigheten inte vara skyldig att begränsa behandlingen av personuppgifterna enligt artikel 18 i dataskyddsförordningen. Avgränsningen till arkivmaterial som tagits emot för förvaring av myndigheten innebär, precis som i 7 a § arkivförordningen, att undantagen inte är tillämpliga avseende personuppgifter i arkivmaterial som härrör från arkivmyndighetens

egen verksamhet. Beslut med stöd av dessa nya bestämmelser bör kunna överklagas på samma sätt som beslut enligt 7 a § arkivförordningen.

Den omständigheten att arkivmyndigheten inte behöver komplettera personuppgifter innebär inte ett förbud mot att göra detta eller vidta någon liknande åtgärd, om arkivmyndigheten bedömer att det är lämpligt. Detta förutsätter dock att åtgärden inte medför en otillåten förvanskning av allmänna handlingar eller en otillåten inskränkning av var och ens rätt att ta del av sådana handlingar.

Det bör noteras att de föreslagna undantagen får tillämpas endast under förutsättning att de direkt tillämpliga villkoren i artikel 89.1 i dataskyddsförordningen om bland annat skyddsåtgärder och uppgiftsminimering efterlevs.

I sammanhanget bör nämnas att rätten till radering, som också framgår av 28 § PUL, regleras i artikel 17 i dataskyddsförordningen. Enligt den direkt tillämpliga bestämmelsen i artikel 17.3 d gäller dock inte denna rätt vid behandling för arkivändamål av allmänt intresse, i den utsträckning som rätten sannolikt omöjliggör eller avsevärt försvårar uppnåendet av syftet med behandlingen.

Anmälningsskyldighet vid rättelse och radering av personuppgifter samt begränsning av behandling

Enligt artikel 19 i dataskyddsförordningen ska den personuppgiftsansvarige underrätta dem som personuppgifter har lämnats ut till, om rättelse, radering eller begränsning sker enligt artiklarna 16–18. Motvarande underrättelseskyldighet regleras i 28 § andra meningen PUL. I denna bestämmelse anges att underrättelse inte behöver lämnas, om det visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats. Ett näst intill likalydande undantag från underrättelseskyldigheten gäller även enligt artikel 19 i dataskyddsförordningen. Undantaget innebär till exempel att en myndighet inte behöver informera dem som har tagit del av en allmän handling om att behandlingen av uppgifter i handlingen har begränsats. Något ytterligare undantag, utöver den i förordningen direkt tillämpliga bestämmelsen, behöver enligt vår bedömning inte införas i svensk rätt. Vi lämnar därför inget sådant förslag.

Rätten till dataportabilitet

Artikel 20 i dataskyddsförordningen, som saknar motsvarighet i personuppgiftslagen, anger att den registrerade under vissa förutsättningar ska ha rätt att få ut de personuppgifter som rör honom eller henne i ett strukturerat, allmänt använt och maskinläsbart format och har rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig. Rätten till dataportabilitet gäller endast om den personuppgiftsansvariges behandling grundar sig på den registrerades samtycke eller är nödvändig för att fullgöra ett avtal med den registrerade. Rätten gäller alltså inte i fråga om en behandling som är nödvändig för att utföra en uppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den personuppgiftsansvarige. Rätten till dataportabilitet skulle därmed endast undantagsvis kunna åberopas avseende personuppgifter som bevarats med stöd av arkivlagstiftningen.

Därtill kommer att rätten till dataportabilitet inte innebär en rätt till radering, se skäl 68. Den personuppgiftsansvarige kan alltså tillgodose den registrerades rätt genom att tillhandahålla en kopia av materialet. I den mån rätten till dataportabilitet alls skulle kunna aktualiseras i arkivmyndigheternas verksamhet skulle utövandet av denna rätt därmed inte påverka myndighetens möjlighet att uppfylla arkivändamålet. Det finns mot denna bakgrund inget skäl att införa något undantag från rätten till dataportabilitet vid behandling av personuppgifter för arkivändamål av allmänt intresse. Vi lämnar därför inte något sådant förslag.

Rätten att göra invändningar

Dataskyddsdirektivets motsvarighet till artikel 21 i dataskyddsförordningen, rörande rätten att göra invändningar, är genomförd i personuppgiftslagen endast såvitt avser direkt marknadsföring, 11 § PUL. Något undantag från denna relativt begränsade rätt att göra invändningar har inte gjorts i personuppgiftslagen.

Rätten att göra invändningar enligt artikel 21.1 dataskyddsförordningen avser behandling av personuppgifter som grundar sig på artikel 6.1 e eller f. Om en invändning görs får den personuppgiftsansvarige inte längre behandla personuppgifterna, såvida inte denne kan påvisa tvingande berättigade skäl för behandlingen som väger

tyngre än den registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk. Enligt vår bedömning står det klart att arkivlagstiftningen i det enskilda fallet kommer att utgöra ett sådant tvingande och berättigat skäl som väger tyngre än den registrerades intressen, i synnerhet när det gäller behandling av personuppgifter som förekommer i arkivmaterial som har överlämnats till en arkivmyndighet. Mot denna bakgrund bör det i arkivförordningen föreskrivas ett generellt undantag från den registrerades principiella rätt att invända mot en arkivmyndighets behandling av personuppgifter för arkivändamål av allmänt intresse. Undantaget bör dock inte vara tillämpligt avseende personuppgifter i arkivmaterial som härrör från arkivmyndighetens egen verksamhet. Beslut med stöd av det nya undantaget bör kunna överklagas på samma sätt som beslut enligt 7 a § arkivförordningen.

Det bör noteras att det föreslagna undantaget får tillämpas endast under förutsättning att de direkt tillämpliga villkoren i artikel 89.1 i dataskyddsförordningen om bland annat lämpliga skyddsåtgärder och uppgiftsminimering efterlevs.

14.4.6 Organ som bör jämföras med myndigheter

Utredningens förslag: Bestämmelserna i dataskyddslagen om behandling av personuppgifter för arkivändamål av allmänt intresse ska i tillämpliga delar också gälla andra organ än myndigheter, i den mån organets verksamhet omfattas av offentlighetsprincipen och sekretesslagstiftningen.

Enligt 2 kap. 2–5 §§ OSL ska vad som föreskrivs i tryckfrihetsförordningen om rätt att ta del av allmänna handlingar hos myndigheter i tillämpliga delar också gälla hos bland annat kommunala bolag och de organ som anges i bilagan till offentlighets- och sekretesslagen, om handlingarna hör till den verksamhet som nämns där. Dessa organ ska enligt samma bestämmelser jämföras med myndigheter vid tillämpningen av offentlighets- och sekretesslagen. De omfattas även av viss arkivlagstiftning (1–2 a §§ arkivlagen). De överväganden som har gjorts i detta kapitel avseende myndigheter är därmed relevanta också för dessa organ. Vid tillämpningen av dataskyddslagens bestämmelser om behandling av personuppgifter för arkivändamål av allmänt intres-

se ska därför andra organ än myndigheter jämföras med myndigheter, i den mån bestämmelserna i tryckfrihetsförordningen och offentlighets- och sekretesslagen om allmänna handlingar och sekretess gäller i organets verksamhet.

14.5 Överväganden och förslag – statistiska ändamål

14.5.1 Statistik

Ordet statistik avser metoder för att samla in, bearbeta, utvärdera och analysera data eller information. Resultatet av ett sådant arbete, ofta redovisat i numerisk form, benämns också statistik. I dataskyddsförordningen avses med statistiska ändamål varje åtgärd som vidtas för den insamling och behandling av personuppgifter som är nödvändig för statistiska undersökningar eller för framställning av statistiska resultat (skäl 162). Ett statistiskt ändamål innebär, enligt samma skäl, att resultatet av behandlingen inte består av personuppgifter, utan av aggregerade personuppgifter, och att resultatet eller uppgifterna inte används till stöd för åtgärder eller beslut som avser en särskild privatperson.

Behandling av personuppgifter för statistiska ändamål förekommer inom såväl offentlig som privat sektor, både som en självständig verksamhet och som en uppföljande åtgärd till annan verksamhet. Statistiska undersökningar kan också utgöra en integrerad del av ett forskningsprojekt. I sådana projekt bör dock all behandling av personuppgifter bedömas enligt de bestämmelser som gäller vid behandling för forskningsändamål. Detta avsnitt omfattar därmed inte sådan behandling av personuppgifter för statistiska ändamål som sker inom ramen för forskning. Vad som ryms inom begreppet forskning kommer att behandlas av Forskningsdatautredningen.

Framställningen av den officiella statistiken, som ska finnas för allmän information, utredningsverksamhet och forskning, regleras av lagen (2001:99) om den officiella statistiken och förordningen (2001:100) om den officiella statistiken. Dessa författningar reglerar bland annat under vilka förutsättningar känsliga personuppgifter får behandlas och vilken information som den statistikansvariga myndigheten ska lämna. Det står klart att hänvisningarna till personuppgiftslagen måste ändras i författningarna om den officiella statistiken. Det kan inte heller uteslutas att dataskyddsförordningen föranleder

materiella författningsändringar. Det ingår dock inte i vårt uppdrag att utreda behovet av eller föreslå sådana ändringar.

14.5.2 Rättslig grund och tillåten vidarebehandling

Den officiella statistiken och annan reglerad statistik framställs av särskilt utpekade myndigheter, som genom författning har tilldelats en uppgift av allmänt intresse. Personuppgifter kan således samlas in och i övrigt behandlas för detta ändamål, utan samtycke från de registrerade, med stöd av artikel 6.1 e i dataskyddsförordningen.

Statistikprojekt som saknar författningsstöd torde däremot inte kunna anses som en uppgift av allmänt intresse som är fastställd i enlighet med svensk rätt. Framställning av statistik som inte sker som en följd av en uppgift som har fastställts i unionsrätten eller i svensk rätt saknar det rättsliga stöd som krävs för att nödvändig behandling av personuppgifter ska kunna ske på grundval av artikel 6.1 e i dataskyddsförordningen. Rättslig grund för behandlingen måste då i stället sökas någon annanstans. Vid sidan av den officiella statistiken och annan reglerad statistikverksamhet torde därför insamling av personuppgifter för statistiska ändamål kräva samtycke från de registrerade. Samtycke krävs således exempelvis för att ett privaträttsligt organ ska kunna samla in personuppgifter i syfte att genomföra en opinions- eller marknadsundersökning, även om undersökningen i och för sig skulle kunna sägas vara av allmänt intresse. Man kan dock också tänka sig att insamling av personuppgifter för viss privaträttsligt bedriven statistikverksamhet skulle kunna vara tillåten utan samtycke, med stöd av en intresseavvägning med stöd av artikel 6.1 f i dataskyddsförordningen.

Dataskyddsförordningen kan således medföra vissa inskränkningar av möjligheterna att, utanför den reglerade statistikverksamheten, samla in personuppgifter för rent statistiska ändamål, jämfört med vad som gäller enligt personuppgiftslagen. Det är inte längre tillräckligt att ett statistikprojekt är av allmänt intresse för att insamling av personuppgifter ska kunna ske utan samtycke från de registrerade – behandlingen måste också vara nödvändig för att utföra en uppgift som är fastställd i unionsrätten eller den nationella rätten. Dessutom kan en intresseavvägning inte längre åberopas som rättslig grund för myndigheter när de fullgör sina uppgifter.

Det är mycket vanligt att personuppgifter som ursprungligen har samlats in för helt andra ändamål vidarebehandlas för statistiska ändamål, t.ex. som ett led i den personuppgiftsansvariges uppföljning av sin egentliga verksamhet. Sådan vidarebehandling är särskilt gynnad i dataskyddsförordningen, precis som i personuppgiftslagen. Uppgifter som ursprungligen samlats in för något annat ändamål kan alltså även i fortsättningen användas för statistiska ändamål, utan att denna nya behandling ska anses vara oförenlig med de ursprungliga ändamålen (artikel 5.1 b i dataskyddsförordningen). En nyhet jämfört med personuppgiftslagen är att det vid sådan vidarebehandling inte krävs någon annan separat rättslig grund än den med stöd av vilken insamlingen av personuppgifter medgavs (skäl 50).

14.5.3 Känsliga personuppgifter

Utredningens förslag: Känsliga personuppgifter ska få behandlas för statistiska ändamål om samhällsintresset av det statistikprojekt där behandlingen ingår klart väger över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan innebära.

Behandling av känsliga personuppgifter för statistiska ändamål får enligt artikel 9.2 j i dataskyddsförordningen ske på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen. Detta utrymme för undantag från förbudet mot behandling av känsliga personuppgifter aktualiseras både vid insamling av personuppgifter för statistiska ändamål och vid vidarebehandling av uppgifter för sådana ändamål.

Vidarebehandling av personuppgifter för statistiska ändamål ska enligt artikel 5.1 b i dataskyddsförordningen visserligen inte anses vara oförenlig med de ursprungliga ändamålen. Känsliga personuppgifter kan däremot inte vidarebehandlas för statistiska ändamål enbart på grundval av det undantag från förbudet som tillämpats vid behandling enligt det ursprungliga ändamålet. Detta följer av att artikel 9.2 j i förordningen förutsätter att gällande rätt innehåller

bestämmelser om lämpliga och särskilda skyddsåtgärder för att säkerställa den registrerades rättigheter och intressen.

Enligt 19 § andra stycket PUL får känsliga personuppgifter behandlas för statistikändamål, om behandlingen är nödvändig på sätt som sägs i 10 § och om samhällsintresset av det statistikprojekt där behandlingen ingår klart väger över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan innebära. I 19 § tredje stycket PUL anges att förutsättningarna enligt andra stycket ska anses uppfyllda om behandlingen har godkänts av en forsknings-etisk kommitté, dvs. ett sådant särskilt organ för prövning av forskningsetiska frågor som har företrädare för såväl det allmänna som forskningen och som är knutet till ett universitet eller en högskola eller till någon annan instans som i mera betydande omfattning finansierar forskning.

I förarbetena till 19 § andra stycket PUL anges att viss statistik är så viktig att den inte bör vara beroende av att varje berörd enskild har informerats och lämnat sitt samtycke. Vidare framgår att det mot bakgrund av det finns många olikartade statistikprojekt, vilka som regel pågår bara under en begränsad tid, förefaller lämpligare att göra en avvägning i varje särskilt fall än att i lag införa generella regler om vilken statistik som ska tillåtas. Vid en sådan individuell avvägning kan olika faktorer kring projektet, t.ex. hur pass viktig den kunskap är som projektet kan ge, vägas mot intrånget i den enskildes personliga integritet.¹⁰

Även vi anser att det inte är lämpligt att genom lagstiftning på förhand avgöra exakt i vilka fall behandling av känsliga personuppgifter ska få ske för statistiska ändamål. Vi föreslår därför att det i dataskyddslagen införs en avvägningsnorm motsvarande den som finns i 19 § andra stycket PUL. Nödvändig behandling av känsliga personuppgifter för statistiska ändamål ska således få ske om samhällsintresset av det statistikprojekt där behandlingen ingår klart väger över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan innebära. För att denna bestämmelse ska aktualiseras förutsätts givetvis att insamlingen av personuppgifter är tillåten med stöd av någon av de rättsliga grunderna i artikel 6.1 i dataskyddsförordningen eller att behandlingen utgör en tillåten vidarebehandling av för andra ändamål insamlade personuppgifter.

¹⁰ Prop. 1997/98:44 s. 71.

Som tidigare har nämnts anser vi att sådana statistiska undersökningar som utgör en integrerad del av ett forskningsprojekt ska bedömas enligt de bestämmelser som gäller för behandling av personuppgifter för forskningsändamål. Den avvägningsnorm som föreslås i detta avsnitt kommer därmed endast att vara tillämplig vid behandling av personuppgifter inom ramen för andra slags statistikprojekt, t.ex. vid framställning av verksamhetsstatistik. Sådan statistik, som alltså saknar samband med ett forskningsprojekt, torde inte komma att prövas av en forskningsetisk kommitté. Det saknas därför skäl att i dataskyddslagen införa en motsvarighet till 19 § tredje stycket PUL.

14.5.4 Lämpliga skyddsåtgärder

Utredningens förslag: Personuppgifter som enbart behandlas för statistiska ändamål ska få användas för att vidta åtgärder i fråga om den registrerade bara om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen. Användningsbegränsningen ska gälla även för myndigheters användning av statistikuppgifter.

Behandling av personuppgifter för statistiska ändamål ska enligt artikel 89.1 i dataskyddsförordningen omfattas av lämpliga skyddsåtgärder för den registrerades rättigheter och friheter. Denna bestämmelse, som är direkt tillämplig, måste den personuppgiftsansvarige följa. För att behandling av känsliga personuppgifter ska vara tillåten för statistiska ändamål krävs dessutom, enligt artikel 9.2 j i dataskyddsförordningen, att unionsrätten eller den nationella rätten innehåller bestämmelser som sådana åtgärder.

I avsnitt 14.5.3 har vi föreslagit att dataskyddslagen ska förse med en bestämmelse som tillåter behandling av känsliga personuppgifter för statistiska ändamål, under vissa förutsättningar. Förslaget, som har utformats enligt den modell som gäller enligt 19 § andra stycket PUL, innefattar ett krav på att samhällsintresset av det statistikprojekt där behandlingen ingår klart ska väga över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan innebära. Det föreslagna villkoret kan i sig sägas utgöra en skyddsåtgärd i dataskyddsförordningens mening.

I avsnitt 14.4.4 angående behandling av personuppgifter för arkivändamål har vi redogjort för vårt förslag att dataskyddslagen ska inne-

hålla en begränsning som motsvarar 9 § fjärde stycket PUL, när det gäller möjligheterna att vidta åtgärder i fråga om den registrerade. En sådan användningsbegränsning bör även gälla i fråga om personuppgifter som endast behandlas för statistiska ändamål. Personuppgifter som enbart behandlas för statistiska ändamål ska därför få användas för att vidta åtgärder i fråga om den registrerade bara om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen. Det saknas även här skäl att ange att uppgifter får användas med den registrerades samtycke. Någon saklig skillnad mellan vårt förslag och 9 § fjärde stycket PUL är inte avsedd.

Begränsningen i 9 § fjärde stycket PUL gäller inte vid myndigheters användning av uppgifter i allmänna handlingar (8 § andra stycket PUL). Undantaget motiveras i förarbetena med att det för sådana personuppgifter redan finns lämpliga skyddsåtgärder i form av bestämmelser om sekretess och skydd för arkiv.¹¹ En allmän utgångspunkt för behandling av personuppgifter för statistiska ändamål är emellertid att resultatet eller uppgifterna inte används till stöd för åtgärder eller beslut som avser en särskild fysisk person (skäl 162). Enligt vår mening står det klart att det finns vissa undantagssituationer då uppgifter som annars bara behandlas för statistiska ändamål måste kunna användas även för att vidta sådana åtgärder, nämligen då den registrerades egna vitala intressen står på spel. I övrigt bör däremot inte heller myndigheter kunna använda uppgifterna för att vidta åtgärder i förhållande till den registrerade. Den omständigheten att uppgifterna finns i allmänna handlingar, eftersom dessa ännu inte hunnit anonymiseras eller gallras, föranleder ingen annan bedömning. Myndigheter bör därför inte undantas från den föreslagna användningsbegränsningen. Om det inom något verksamhetsområde eller för någon viss myndighet skulle finnas behov av ett sådant undantag bör det övervägas särskilt.

¹¹ Prop. 1997/98:44 s. 63.

14.5.5 Undantag från vissa av den registrerades rättigheter

Utredningens bedömning: Dataskyddslagen bör inte innehålla något generellt undantag från de registrerades rättigheter vid behandling för statistiska ändamål.

I avsnitt 14.3.1 har vi redogjort för artikel 14.5 b och 17.3 d i dataskyddsförordningen, som utgör direkt tillämpliga undantag från vissa av förordningens bestämmelser om de registrerades rättigheter. Om personuppgifter behandlas för statistiska ändamål får det dessutom, enligt artikel 89.2, i nationell rätt föreskrivas undantag från de rättigheter som avses i artiklarna 15, 16, 18 och 21, med förbehåll för de villkor och skyddsåtgärder som avses i artikel 89.1. Detta får emellertid bara göras i den utsträckning som sådana rättigheter sannolikt kommer att göra det omöjligt eller mycket svårare att uppfylla det särskilda ändamålet och sådana undantag krävs för att uppnå detta ändamål.

Vi kan konstatera att det är mycket svårt att överblicka behovet och konsekvenserna av ett generellt undantag från de registrerades rättigheter vid behandling av personuppgifter för statistiska ändamål. Vi anser därför att dataskyddslagen inte bör innehålla någon sådan bestämmelse. Vid behov, och om det bedöms vara lämpligt, bör sådana undantag i stället införas i sektorsspecifika författningar.

Enligt 19 § fjärde stycket PUL får personuppgifter lämnas ut för att användas i sådana statistikprojekt som avses i 19 § andra stycket PUL, om inte något annat följer av regler om sekretess och tystnadsplikt. Bestämmelsen innebär ingen skyldighet, endast en möjlighet, att lämna ut uppgifter. Av förarbetena framgår att bestämmelsens syfte och konsekvens är att den statistiker som hämtar in uppgifter från någon annan än de registrerade inte behöver informera de registrerade om sin behandling. Bestämmelsen medför nämligen att det undantag från informationsplikten som föreskrivs i 24 § andra stycket PUL blir tillämpligt.¹² Enligt detta undantag behöver information enligt första stycket samma paragraf inte lämnas, om det finns bestämmelser om registrerandet eller utlämnandet av personuppgifterna i en lag eller någon annan författning.

¹² Prop. 1997/98:44 s. 127.

I artikel 14.5 c i dataskyddsförordningen föreskrivs, på ett likartat sätt som i artikel 11.2 i dataskyddsdirektivet, att informationsplikten enligt artikel 14.1–4 inte gäller om erhållande eller utlämnande av uppgifter uttryckligen föreskrivs genom unionsrätten eller genom en medlemsstats nationella rätt. Dessutom anges i artikel 14.5 b i förordningen att informationsplikten inte gäller vid behandling av personuppgifter för statistiska ändamål, om tillhandahållandet av information visar sig vara omöjligt eller skulle medföra en oproportionell ansträngning eller om skyldigheten sannolikt skulle göra det omöjligt eller avsevärt försvåra uppfyllandet av målen med behandlingen. Enligt vår bedömning fyller den sistnämnda bestämmelsen behovet på generell nivå av undantag från informationsplikten. Vi föreslår därför ingen bestämmelse som motsvarar 19 § fjärde stycket PUL. Bestämmelser som uttryckligen föreskriver att uppgifter ska lämnas ut eller samlas in, och som medför att informationsplikten enligt dataskyddsförordningen inte gäller, bör i stället övervägas på sektors-specifik nivå. Sådana bestämmelser finns redan bland annat i lagen och förordningen om den officiella statistiken.

15 Förhandstillstånd

15.1 Vårt uppdrag

I kommittédirektiven anges att vi ska överväga om regeringen också fortsättningsvis ska ha en generell möjlighet att meddela föreskrifter om krav på förhandstillstånd i vissa fall, eller om sådana föreskrifter endast bör tas in i sådan sektorsspecifik lagstiftning som ligger utanför utredningens uppdrag.

15.2 Gällande rätt

Enligt 41 § PUL har regeringen möjlighet att meddela föreskrifter om att behandlingar som innebär särskilda risker för otillbörligt intrång i den personliga integriteten ska anmälas för förhandskontroll till tillsynsmyndigheten. Bestämmelsen har införts för att genomföra artikel 20.1 i dataskyddsdirektivet. Enligt artikeln ska medlemsstaterna bestämma vilka behandlingar som kan innebära särskilda risker för den registrerades fri- och rättigheter och säkerställa att dessa behandlingar kontrolleras innan de påbörjas. Det är tillsynsmyndigheten som ska utföra förhandskontrollen sedan en anmälan kommit in från den personuppgiftsansvarige eller personuppgiftsombudet. Det har tidigare funnits vissa sådana bestämmelser i personuppgiftsförordningen men dessa har upphävts. Viss behandling som regleras i särskild ordning, t.ex. Skatteverkets behandling av personuppgifter i samband med brottsutredningar, omfattas däremot av bestämmelser om förhandskontroll.¹

¹ 2 § förordningen (1999:105) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar.

15.3 Dataskyddsförordningen

Förhandssamråd regleras i artikel 36 i dataskyddsförordningen, och kommenteras i skäl 94. Av artikeln framgår att den personuppgifts-ansvarige ska samråda med tillsynsmyndigheten före behandling om en konsekvensbedömning visar att behandlingen skulle leda till en hög risk, om inte den personuppgiftsansvarige skulle vidta åtgärder för att minska risken.

Om tillsynsmyndigheten anser att den planerade behandlingen skulle strida mot förordningen, ska tillsynsmyndigheten ge personuppgiftsansvarig och personuppgiftsbiträde skriftliga råd och utnyttja sina befogenheter enligt artikel 58. Det gäller exempelvis att begära information, utfärda varningar om att planerade behandlingar sannolikt kommer att bryta mot förordningen och förelägga den personuppgiftsansvarige om rättelse eller radering.

Vid samråd med tillsynsmyndigheten ska den personuppgifts-ansvarige lämna viss närmare specificerad information, t.ex. ändamålen med och medlen för den avsedda behandlingen, de åtgärder som vidtas och de garantier som lämnas för att skydda de registrerades rättigheter och friheter enligt denna förordning och den genomförda konsekvensutredningen. Underlåtenhet att utföra en konsekvensutredning och att samråda med tillsynsmyndigheten kan föranleda att sanktionsavgift påförs enligt artikel 83.4.

I artikel 36.5 ges medlemsstaterna utrymme att i sin nationella rätt i stället kräva att personuppgiftsansvariga alltid ska samråda med och erhålla förhandstillstånd av tillsynsmyndigheten när det gäller en personuppgiftsansvarigs behandling för utförandet av en uppgift av allmänt intresse, inbegripet behandling avseende social trygghet och folkhälsa.

15.4 Överväganden

Utredningens bedömning: Ett bemyndigande för regeringen att meddela föreskrifter om förhandstillstånd för vissa behandlingar bör inte tas in i dataskyddslagen, utan i de fall det bedöms nödvändigt tas in i sektorsspecifik reglering.

Den enda generella reglering som har antagits med stöd av bemyndigandet i 41 § PUL är den numera upphävda 10 § PUF. Bestämmelsen innebar att automatiserade behandlingar av personuppgifter om genetiska anlag som framkommit efter genetisk undersökning, skulle anmälas för förhandskontroll till Datainspektionen senast tre veckor i förväg. Bestämmelsen upphörde att gälla den 1 mars 2013.

Som nämnts ovan finns föreskrifter om anmälan för förhandskontroll rörande behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar. Tidigare gällde även krav på förhandstillstånd för vissa behandlingar hos andra brottsbekämpande myndigheter, såsom polisen, Kustbevakningen och Tullverket.² När det gäller polisen och Kustbevakningen har kraven på tillstånd numera ersatts av ett samrådsförfarande.³ Det finns vidare en fortsatt möjlighet för regeringen att förordna att viss behandling hos Tullverket kräver förhandstillstånd, genom en hänvisning till 41 § PUL i 6 § första stycket 7 lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet. Möjligheten har dock inte utnyttjats.

Redan Datalagskommittén ansåg att skyldigheten att i förväg anmäla behandlingar till tillsynsmyndigheten för förhandskontroll borde begränsas till ett minimum och att Datainspektionens resurser i stället skulle användas för att ge råd, sprida kunskap och utöva tillsyn.⁴ Datalagskommittén ansåg dock att det skulle vara oförenligt med direktivet att införa en bestämmelse om att inga behandlingar måste kontrolleras på förhand. Det bedömdes som mest lämpligt att regeringen fick meddela sådana föreskrifter på förordningsnivå, varför kommittén föreslog den delegationsbestämmelse som återfinns i 41 § PUL.⁵

Dataskyddsförordningen stadgar en relativt långtgående samråds-skyldighet i kombination med kraftfulla befogenheter och en möjlighet att påföra sanktionsavgift om skyldigheten inte efterlevs. Utvecklingen i svensk rätt har alltmer rört sig mot ett avskaffande av tillståndsförfaranden och en utökad användning av samrådsförfaran-

² Se 2 § i numera upphävda polisdataförordningen (1999:81), 10 § tredje stycket numera upphävda förordningen (2003:188) om behandling av personuppgifter inom Kustbevakningen, och 2 § numera upphävda förordningen (2001:88) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet.

³ Se 2 § polisdataförordningen (2010:1155) och 2 § kustbevakningsdataförordningen (2012:146).

⁴ SOU 1997:39 s. 423 f.

⁵ SOU 1997:39 s. 430.

den. Förordningen ställer, till skillnad från dataskyddsdirektivet, inga krav på att medlemsstaterna ska reglera frågan om förhandstillstånd. Tvärtom är det ett av syftena med att dataskyddsreformen att minska byråkratin genom att avskaffa kravet på anmälningar och tillstånd.⁶ Den möjlighet som medlemsstaterna ges i artikel 36.5 att reglera tillståndsfrågan är rent fakultativ.

Mot denna bakgrund bör skälen för en sådan reglering övervägas noga i varje enskilt fall och anpassas till de speciella förhållanden som råder inom den sektor där behandlingen är tänkt att ske. Vi menar därför att det inte finns skäl att generellt bemyndiga regeringen att meddela föreskrifter om förhandstillstånd. Sådana bemyndiganden får i stället, i de fall det bedöms nödvändigt, tas in i sektorsspecifik lag.

⁶ Europeiska kommissionens pressmeddelande den 15 december 2015 ”Överenskommelse om kommissionens reform av EU:s uppgiftsskydd stärker den digitala inre marknaden”.

16 Godkännande av certifieringsorgan

16.1 Vårt uppdrag

Enligt dataskyddsförordningen ska medlemsstaterna, Europiska dataskyddsstyrelsen och kommissionen, framför allt på unionsnivå, uppmantra till att det införs certifieringsmekanismer och märkningar i syfte att personuppgiftsansvariga och personuppgiftsbiträden ska kunna visa att de uppfyller kraven i förordningen. Sådan certifiering kan utföras av särskilda certifieringsorgan eller av tillsynsmyndigheten. I kommittédirektiven anges att dataskyddsförordningen kräver att medlemsstaterna inför bestämmelser för hur sådana särskilda certifieringsorgan ska godkännas. Det ingår därför i vårt uppdrag att bedöma hur certifieringsorgan ska godkännas och att lämna sådana författningsförslag som är behövliga och lämpliga.

16.2 Dataskyddsförordningen

Enligt artikel 24 i dataskyddsförordningen ska den personuppgiftsansvarige kunna visa att behandlingen utförs i enlighet med denna förordning. Detta kan bland annat ske genom användning av godkända certifieringsmekanismer. Sådana mekanismer kan även användas för att visa att den personuppgiftsansvarige följer kraven i artikel 25 på inbyggt dataskydd och dataskydd som standard, att ett personuppgiftsbiträde tillhandahåller tillräckliga garantier enligt artikel 28, och att lämpliga tekniska och organisatoriska åtgärder vidtas enligt artikel 32.

De godkända certifieringsmekanismer som avses i dessa bestämmelser regleras närmare i artikel 42. Där anges bland annat att medlemsstaterna, tillsynsmyndigheterna, styrelsen och kommissionen ska

uppmuntra, särskilt på unionsnivå, införandet av certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd som syftar till att visa att personuppgiftsansvarigas eller personuppgiftsbitrådets behandling är förenlig med förordningen (punkt 1). Certifieringsförfarandet ska vara frivilligt (punkt 3). Certifiering minskar inte den personuppgiftsansvariges eller personuppgiftsbitrådets ansvar för att förordningen efterlevs och påverkar inte tillsynsmyndigheternas uppgifter och befogenheter (punkt 4). Certifieringar ska utfärdas av särskilda certifieringsorgan, den behöriga tillsynsmyndigheten eller styrelsen (punkt 5).¹

Särskilda certifieringsorgan ska enligt artikel 43 vara ackrediterade. Medlemsstaten ska säkerställa att certifieringsorganen är ackrediterade av både eller endera av tillsynsmyndigheten och det nationella ackrediteringsorgan som utsetts i enlighet med förordning (EG) nr 765/2008². Ackrediteringen ska ske i enlighet med EN-ISO/IEC 17065/2012 och med de ytterligare krav som fastställts av tillsynsmyndigheten. Certifieringsorgan får ackrediteras endast om vissa villkor som anges i artikeln är uppfyllda och på grundval av offentliggjorda kriterier som godkänts av tillsynsmyndigheten eller styrelsen.

Tillsynsmyndigheten tilldelas genom artikel 57.1 i dataskyddsförordningen en rad uppgifter som rör certifieringsmekanismen. Myndigheten ska bland annat

- godkänna certifieringskriterierna (led n),
- genomföra en periodisk översyn av utfärdade certifieringar (led o),
- utarbeta och offentliggöra kriterier för ackreditering av certifieringsorgan (led p), och
- ackreditera certifieringsorgan (led q).

I artikel 58.3 anges att tillsynsmyndigheten ska ha befogenhet att

- ackreditera certifieringsorgan (led e), och
- utfärda certifieringar och godkänna certifieringskriterier (led f).

¹ Det kan dock noteras att uppgiften att utfärda certifiering inte nämns i de artiklar som anger styrelsens uppgifter.

² Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknads kontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93.

16.3 Överväganden

16.3.1 Certifiering, ackreditering och Swedac

Certifiering är ett förfarande som syftar till att bedöma om vissa specificerade krav avseende till exempel en process eller ett organ har uppfyllts. Kraven kan handla om olika aspekter, exempelvis säkerhet eller hälsa. Kraven kan framgå av författning, branschöverenskommelse eller standard.³

Med ackreditering avses ett formellt erkännande att ett organ är kompetent att utföra vissa specificerade tjänster. Ackrediteringen meddelas av ett särskilt ackrediteringsorgan efter genomförd utvärdering. Ackreditering syftar till att bedöma och säkerställa att tillämpliga krav uppfylls. I svensk lagstiftning som inte härrör från unionslagstiftning, dvs. som ligger utanför det harmoniserade området, krävs ofta ackreditering för organ som utför kontroll, certifiering och liknande tjänster.⁴

Styrelsen för ackreditering och teknisk kontroll (Swedac) har utsetts att vara nationellt ackrediteringsorgan i Sverige och ansvarar för ackreditering enligt förordning (EG) nr 765/2008. Swedac ansvarar enligt lagen (2011:791) om ackreditering och teknisk kontroll även för ackreditering i övrigt av organ för bedömning av överensstämmelse. Även vid sådan ackreditering ska vissa bestämmelser i förordning (EG) nr 765/2008 tillämpas. Ett organ som vill bli ackrediterat måste lämna en ansökan till Swedac som prövar och bedömer om organet uppfyller de krav som ställs. Förfaranderegler finns i förordningen (2011:811) om ackreditering och teknisk kontroll.

16.3.2 Vår bedömning

Utredningens bedömning: Det bör för närvarande inte införas några ytterligare bestämmelser om hur certifieringsorgan ska godkännas.

³ Prop. 2010/11:80 s. 40.

⁴ Prop. 2010/11:80 s. 42.

I kommittédirektiven anges att dataskyddsförordningen kräver att medlemsstaterna inför bestämmelser för hur särskilda certifieringsorgan ska godkännas. Av förordningens slutliga lydelse är det emellertid svårt att utläsa något sådant krav.

I artikel 43.1 anges att medlemsstaterna ska säkerställa att certifieringsorgan är ackrediterade av antingen tillsynsmyndigheten eller av det nationella ackrediteringsorganet eller av båda dessa. Frågan är vad som avses med uttrycket ”säkerställa” i detta sammanhang. I den engelska språkversionen används uttrycket *ensure*. En möjlig tolkning är att det ankommer på medlemsstaten att se till att de certifieringsorgan som verkar på marknaden är ackrediterade. Detta bör dock snarare vara en uppgift för tillsynsmyndigheten, än för staten som sådan. En rimligare tolkning, som dock ligger längre från bestämmelsens ordalydelse, är att staten är skyldig att se till att antingen tillsynsmyndigheten eller det nationella ackrediteringsorganet eller att dessa båda organ har de befogenheter och verktyg som behövs för att ackreditera certifieringsorgan.

Tillsynsmyndighetens uppgift och befogenhet att ackreditera certifieringsorgan anges uttryckligen i artiklarna 57.1 q och 58.3 e. Ett organ som vill bli ackrediterat måste därmed anses ha en direkt på förordningen grundad rätt att få sin överensstämmelse med kraven bedömda av tillsynsmyndigheten. Det kan mot denna bakgrund inte komma i fråga att genom nationell lagstiftning vare sig tilldela eller frånta tillsynsmyndigheten denna uppgift.

Swedac är i Sverige det nationella ackrediteringsorgan som utpekats i artikel 43.1 b. Swedac ansvarar enligt sin instruktion⁵ även för annan ackrediteringsverksamhet än den som avses i förordning (EG) nr 765/2008. Det regelverk som på nationell nivå kompletterar förordning (EG) nr 765/2008, till exempel avseende förfarandet, är tillämpligt även på sådan annan ackrediteringsverksamhet. För det fall att ett organ som vill bli ackrediterat skulle anses ha en direkt på förordningen grundad rätt att få sin överensstämmelse med kraven bedömda av det nationella ackrediteringsorganet torde det således inte behövas några ytterligare författningsåtgärder.

Det kan noteras att det i artikel 70.1 o anges att även Europeiska dataskyddsstyrelsen, på eget initiativ eller på begäran av kommis-

⁵ Förordningen (2009:895) med instruktion för Styrelsen för ackreditering och teknisk kontroll.

sionen, ska ackreditera certifieringsorgan. Det får förutsättas att avsikten är att en ackreditering som beslutats av styrelsen ska fylla samma självständiga funktion som annan ackreditering enligt data-skyddsförordningen. Mot den bakgrunden framstår medlemsstaternas skyldighet enligt artikel 43.1 att ”säkerställa” att certifieringsorgan är ackrediterade av både eller endera av tillsynsmyndigheten och det nationella ackrediteringsorganet som än mer svårångad. Det kan även av detta skäl ifrågasättas om det krävs några ytterligare bestämmelser i svensk rätt för hur certifieringsorgan ska godkännas.

Enligt artiklarna 43.8 och 43.9 får kommissionen anta delegerade akter och genomförandeakter rörande bland annat certifieringsmekanismen. Förhoppningsvis klarnar rättsläget genom dessa rättsakter. I avvaktan på att kommissionen antar sådana akter, och med tanke på att i vart fall tillsynsmyndigheten redan genom förordningens direkt tillämpliga bestämmelser har rätt och skyldighet att ackreditera certifieringsorgan, lämnar vi inte några författningsförslag om hur certifieringsorgan ska godkännas.

17 Sekretess

17.1 Vårt uppdrag

Dataskyddsförordningen innehåller bestämmelser om tystnadsplikt och konfidentialitet hos tillsynsmyndigheten och för dataskyddsombud. I båda fallen hänvisar förordningen till nationell rätt. Offentlighets- och sekretesslagen innehåller dels en bestämmelse om sekretess hos Datainspektionen som aktualiseras i detta sammanhang, dels flera bestämmelser som hänvisar till personuppgiftslagen. Dessa bestämmelser måste ses över med anledning av den nya regleringen i förordningen och personuppgiftslagens upphävande.

Vårt uppdrag när det gäller sekretessfrågor har tre delar. Vi ska för det första analysera om nuvarande sekretessbestämmelser behöver anpassas med anledning av förordningens reglering om tystnadsplikt hos tillsynsmyndigheten. För det andra ska vi analysera vilken reglering som behöver införas i svensk rätt med anledning av förordningens bestämmelser om sekretess och tystnadsplikt för dataskyddsombud. Slutligen ska vi överväga hur de bestämmelser i offentlighets- och sekretesslagen som innehåller hänvisningar till personuppgiftslagen bör anpassas till den nya regleringen.

17.2 Allmänt om grundlags- och sekretessregleringen

Offentlighetsprincipen innebär att allmänheten och massmedierna ska ha insyn i statens och kommunernas verksamhet. Offentlighetsprincipen kommer till uttryck på olika sätt, exempelvis genom yttrande- och meddelarfrihet för tjänstemän, genom domstolsoffentlighet och genom offentlighet vid beslutande församlingars sammanträden. När det mer allmänt talas om offentlighetsprincipen brukar man i första hand syfta på reglerna om allmänna handlingars offentlighet. Dessa regler finns i tryckfrihetsförordningens andra kapitel.

Enligt 2 kap. 2 § första stycket tryckfrihetsförordningen får rätten att ta del av allmänna handlingar begränsas endast om det är påkallat med hänsyn till vissa angivna intressen, däribland enskilda personliga eller ekonomiska förhållanden. En sådan begränsning ska enligt andra stycket anges noga i en bestämmelse i en särskild lag eller, om det i ett visst fall är lämpligare, i en annan lag vartill den särskilda lagen hänvisar. Efter bemyndigande i en sådan bestämmelse får regeringen genom förordning meddela närmare föreskrifter om bestämmelsens tillämplighet.

Med handling förstås enligt 2 kap. 3 § första stycket tryckfrihetsförordningen en framställning i skrift eller bild samt en upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel. Handlingsbegreppet i tryckfrihetsförordningen omfattar således även sådan automatiserad behandling som avses i personuppgiftslagen och dataskyddsförordningen.

En handling är allmän om den förvaras hos en myndighet och enligt 2 kap. 6 eller 7 § tryckfrihetsförordningen är att anse som inkommen till eller upprättad hos en myndighet. En upptagning ska enligt 2 kap. 3 § andra stycket tryckfrihetsförordningen anses vara förvarad hos en myndighet om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas. En handling som förvaras hos en myndighet endast som led i teknisk bearbetning eller teknisk lagring för annans räkning anses enligt 2 kap. 10 § tryckfrihetsförordningen inte som allmän handling hos den myndigheten.

Offentlighets- och sekretesslagen utgör i dag den särskilda lag som avses i 2 kap. 2 § andra stycket tryckfrihetsförordningen. Regeringen har meddelat närmare tillämpningsföreskrifter i offentlighets- och sekretessförordningen (2009:641).

Sekretess innebär enligt 3 kap. 1 § OSL ett förbud att röja en uppgift, oavsett om det sker genom utlämnande av en handling eller genom att röja uppgiften muntligen eller på något annat sätt. Sekretessen innebär således dels handlingssekretess, dels tystnadsplikt. Av 2 kap. 2–4 § OSL framgår att riksdagen, beslutande kommunala församlingar och sådana organ som avses i 2 kap. 3 och 4 §§ OSL ska jämföras med myndighet vid tillämpning av offentlighets- och sekretesslagen. Bestämmelser om tystnadsplikt finns också utanför offent-

lighets- och sekretesslagens tillämpningsområde, exempelvis för anställda inom den privata hälso- och sjukvården och för advokater.

17.3 Sekretess hos tillsynsmyndigheten

17.3.1 Gällande rätt

Enligt artikel 28.7 i dataskyddsdirektivet ska medlemsstaterna föreskriva att tillsynsmyndighetens ledamöter och personal, även sedan deras anställning upphört, ska ha tystnadsplikt med avseende på förtrolig information som de har tillgång till.

Enligt 32 kap. 1 § OSL gäller sekretess hos Datainspektionen bland annat i ärende om tillstånd eller tillsyn som enligt lag eller annan författning ska handläggas av inspektionen för uppgift om en enskilds personliga eller ekonomiska förhållanden, om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs.

Sekretessen gäller till skydd för uppgifter om en enskilds personliga eller ekonomiska förhållanden och omfattar alltså såväl uppgifter om fysiska personer, till exempel uppgifter om registrerade i ett kund- eller ärendehandläggningssystem, som uppgifter som hänför sig till näringsidkares affärs- eller driftförhållanden. Det har också ansetts att sekretess till skydd för enskilds personliga och ekonomiska förhållanden kan gälla det faktum att det är en viss person som har lämnat vissa uppgifter. Uppgifter som lämnas till en myndighet och som indirekt kan avslöja en uppgiftslämnarens identitet på grund av att bara en viss person eller befattningshavare kan ha kännedom om dem kan också omfattas av sekretessen om de kan röja den enskildes identitet.¹

Sekretessen i 32 kap. 1 § OSL gäller med ett så kallat rakt skaderekvisit. Det innebär att en presumtion för offentlighet gäller. Ett rakt skaderekvisit innebär normalt att det är uppgifternas karaktär som får avgöra om sekretess gäller eller inte. Avsikten är att skadebedömningen i dessa fall i huvudsak ska kunna göras med utgångspunkt i själva uppgiften. Frågan om sekretess gäller behöver därmed inte i första hand knytas till en skadebedömning i det enskilda

¹ Lenberg m.fl., Offentlighets- och sekretesslagen (8 november 2016, Zeteo), kommentaren till 32 kap. 8a § OSL.

fallet. Avgörande bör i stället vara om uppgiften är av den arten att ett utlämnande typiskt sett kan vara ägnat att medföra skada för det intresse som ska skyddas genom bestämmelsen. Om uppgiften är sådan att den genomsnittligt sett måste betraktas som harmlös ska den alltså normalt anses falla utanför sekretessen. Om uppgiften i stället typiskt sett måste betraktas som känslig omfattas den normalt av sekretess.² Det har förutsatts att skaderekvisitet i 32 kap. 1 § OSL får tolkas med beaktande av den sekretess som gäller för personuppgifterna i verksamheten hos den myndighet uppgifterna kommer ifrån³, och att paragrafen vid behov bör tolkas unionskonformt i förhållande till direktivets krav på tystnadsplikt.⁴ Sekretessens räckvidd enligt bestämmelsen begränsas till ärende om tillstånd eller tillsyn som enligt lag eller annan författning ska handläggas av Datainspektionen. Sekretessen gäller i högst sjuttio år för uppgifter i allmänna handlingar.

Bestämmelsen i 11 kap. 1 § första stycket OSL om överföring av sekretess i tillsynsverksamhet är i praktiken inte tillämplig på Datainspektionens uppgifter när det gäller sekretess till skydd för enskildas förhållanden, eftersom det i 11 kap. 8 § samma lag föreskrivs att bestämmelserna om överföring av sekretess inte gäller om uppgiften hos den mottagande myndigheten redan omfattas av en annan bestämmelse till skydd för samma intresse.

Då det gäller sekretess till skydd för andra intressen tillämpas bestämmelserna i 15–19 kap. OSL. Exempelvis skulle bestämmelserna om utrikessekretess i 15 kap. 1 § och om sekretess i det internationella samarbetet i 15 kap. 1a § kunna bli tillämpliga i vissa situationer, liksom sekretessen till skydd för inspektionsförberedelser i 17 kap. 1 § och sekretessen till skydd för säkerhets- eller bevakningsåtgärd avseende system för automatiserad behandling av information i 18 kap. 8 § 3.

² Prop. 1979/80:2 Del A s. 80 f.

³ Lenberg m.fl., Offentlighets- och sekretesslagen (8 november 2016, Zeteo), kommentaren till 32 kap. 1 § OSL.

⁴ Prop. 1997/98:44 s. 146.

17.3.2 Dataskyddsförordningen

Enligt artikel 54.2 i dataskyddsförordningen ska varje tillsynsmyndighets ledamöter och personal, i enlighet med unionsrätten eller medlemsstaternas nationella rätt, omfattas av tystnadsplikt både under och efter sin mandattid vad avser konfidentiell information som de fått kunskap om under utförandet av deras uppgifter eller utövandet av deras befogenheter. Under mandatperioden ska tystnadsplikten i synnerhet gälla rapportering från fysiska personer om överträdelser av förordningen.

17.3.3 Överväganden

Utredningens bedömning: Någon förändring av den befintliga sekretessbestämmelsen till skydd för enskildas personliga och ekonomiska förhållanden i Datainspektionens verksamhet krävs inte till följd av dataskyddsförordningens reglering om tystnadsplikt för ledamöter och personal hos tillsynsmyndigheten.

Utredningen om tillsynen över den personliga integriteten har i betänkandet SOU 2016:65 föreslagit att Datainspektionen ska vara tillsynsmyndighet enligt dataskyddsförordningen och att detta ska framgå av förordningen (2007:975) med instruktion för Datainspektionen. Våra direktiv är också skrivna med denna utgångspunkt. De fortsatta resonemangen kommer därför att utgå från detsamma.

Dataskyddsförordningen innehåller inga skäl som skulle kunna ge ledning för den närmare tolkningen av artikel 54.2. Artikelns ordalydelse antyder dock att det främst är sekretess till skydd för enskildas personliga och ekonomiska förhållanden som avses och inte sekretess till skydd för t.ex. tillsynsmyndighetens verksamhet. Hänvisningen till medlemsstaternas nationella rätt och begränsningen till konfidentiell information gör enligt vår bedömning att medlemsstaterna har relativt stort utrymme att utforma en lämplig reglering.

Det är framför allt bestämmelsen i 32 kap. 1 § OSL som reglerar skyddet för enskildas personliga och ekonomiska förhållanden hos Datainspektionen. I artikel 54.2 används termen tystnadsplikt och att denna ska gälla både under och efter ledamöters och personals mandattid. Som nämnts ovan innebär bestämmelser om sekretess i offent-

lighets- och sekretesslagen både handlingssekretess och tystnadsplikt. Sekretessen enligt 32 kap. 1 § OSL gäller i upp till sjuttio år. Av 2 kap. 1 § OSL framgår att en befattningshavare som är skyldig att iaktta sekretess också är det sedan han eller hon har lämnat sin befattning.⁵

Om uppgifter har lämnats till Datainspektionen från en tillsynsmyndighet i någon annan medlemsstat inom ramen för det samarbete som förutsätts i förordningen sker detta i ärende om tillstånd eller tillsyn som enligt lag eller annan författning ska handläggas av inspektionen och omfattas därmed av sekretessen i 32 kap. 1 § OSL. Det kan också noteras att sekretessen gäller även för företrädare för tillsynsmyndigheter i andra medlemsstater som enligt artikel 62.3 i förordningen förordnats att utföra vissa uppgifter eller att inom ramen för vissa angivna befogenheter annars agera för den svenska tillsynsmyndighetens räkning, så länge kraven i 2 kap. 1 § OSL är uppfyllda.

Med den tolkning bestämmelsen har fått i svensk rätt bedömer vi att den utgör ett tillräckligt sådant skydd för enskildas personliga och ekonomiska förhållanden som förutsätts i förordningen. Det har inte heller framkommit något under utredningen som talar för att bestämmelsen om sekretess i Datainspektionens verksamhet har förorsakat tillämpningssvårigheter eller att sekretessen skulle vara otillräcklig ur ett integritetsperspektiv.

Datainspektionens uppgift att handlägga tillsynsärenden enligt dataskyddsförordningen kommer att framgå av myndighetens instruktion. Därmed regleras inspektionens tillsynsverksamhet enligt dataskyddsförordningen i författning på det sätt som förutsätts i 32 kap. 1 § OSL. Några förändringar i bestämmelsens ordalydelse bedöms därför inte nödvändiga.

I detta sammanhang kan det förtjäna att påpekas att den incidentrapportering som förutsätts ske till tillsynsmyndigheten i enlighet med artikel 33 i förordningen, i praktiken kan innebära en upplysning om att ingivarens it-system är sårbart för attacker. Uppgiften om vem som har lämnat in en sådan rapport kan alltså innebära en säkerhetsrisk. Uppgifter om ingivare av incidentrapportering avseende säkerhetsbrister i it-system till Post- och telestyrelsen, liksom uppgifter om innehållet i rapporterna, har i ett tidigare lagstiftningsärende ansetts omfattas av sekretessen till skydd för säkerhets- och bevak-

⁵ Lenberg m.fl., Offentlighets- och sekretesslagen (8 november 2016, Zeteo), kommentaren till 2 kap. 1 § OSL.

ningsåtgärder avseende system för automatiserad behandling av information i 18 kap. 8 § OSL.⁶ Vår bedömning är att motsvarande skydd kommer att gälla för uppgifter som rör incidentrapportering enligt förordningens artikel 33. I vilken mån den uppgiften kan hemlighållas i diariet får bedömas enligt 5 kap. 2 § och 18 kap. 8 § OSL.⁷

17.4 Tystnadsplikt för dataskyddsombud

17.4.1 Gällande rätt

I dataskyddsdirektivet finns bestämmelserna om motsvarigheten till förordningens dataskyddsombud i artikel 18 andra och tredje strecksatserna. Där framgår att en anmälan om behandling till tillsynsmyndigheten kan underlåtas om den registeransvarige i enlighet med nationell lagstiftning utser ett uppgiftsskyddsombud. Ombudet ska bland annat ha till uppgift att på ett oberoende sätt säkerställa den interna tillämpningen av de nationella bestämmelser som antagits till följd av direktivet. I direktivet finns inga bestämmelser om tystnadsplikt eller sekretess för uppgiftsskyddsombud.

Direktivets bestämmelser har implementerats i svensk rätt genom bestämmelserna om personuppgiftsombud i 38–40 §§ PUL. Inte heller i svensk rätt finns någon särskild reglering om tystnadsplikt för personuppgiftsombud.

17.4.2 Dataskyddsförordningen

Ett dataskyddsombud ska enligt förordningen ha till uppgift att informera de personuppgiftsansvariga, biträden och anställda om skyldigheterna enligt förordningen och andra unions- eller medlemsstatsreglerade dataskyddsbestämmelser. Ombudet ska också bland annat övervaka efterlevnaden av förordningen och samarbeta med tillsynsmyndigheten (artikel 39).

⁶ Prop. 2003/04:93 s. 82.

⁷ Utredningen om genomförande av NIS-direktivet, Ju 2016:11, har i uppdrag att överväga om det nuvarande sekretessskyddet för rapportering av it-incidenter i 18 kap. 8 § OSL är tillräckligt och att annars föreslå ändringar i offentlighets- och sekretesslagen för att känslig information i incidentrapporter ska kunna skyddas (dir. 2016:29).

Myndigheter som behandlar personuppgifter måste utnämna dataskyddsbud. Detsamma gäller personuppgiftsansvariga eller biträden som utför behandling där omfattningen, ändamålen eller uppgifternas karaktär motiverar att ett ombud utses (artikel 37). I artiklarna 37.5 och 38 finns bestämmelser om dataskyddsbudets kvalifikationer och ställning. I artikel 37.6 stadgas att dataskyddsbudet får ingå i den personuppgiftsansvariges eller bitrådets personal, eller utföra uppgifterna på grundval av ett tjänsteavtal. Av sammanhanget framgår alltså tydligt att ombudet ska vara en fysisk person. Flera myndigheter eller flera bolag i en koncern kan ha ett gemensamt dataskyddsbud under vissa förutsättningar (artikel 37.2–3).

Enligt artikel 38.5 ska dataskyddsbudet, när det gäller dennes genomförande av sina uppgifter, vara bundet av sekretess eller konfidentialitet i enlighet med unionsrätten eller medlemsstaternas nationella rätt.

17.4.3 Överväganden och förslag

Utredningens förslag: Den som utsetts till dataskyddsbud enligt dataskyddsförordningen ska inte obehörigen få röja det som han eller hon vid fullgörandet av sin uppgift har fått veta om enskilds personliga eller ekonomiska förhållanden.

Utredningens bedömning: I det allmännas verksamhet är regleringen i offentlighets- och sekretesslagen tillräcklig för att uppfylla kraven på tystnadsplikt för dataskyddsbud enligt förordningen.

Bakgrund

Regleringen i offentlighets- och sekretesslagen är detaljerad och differentierad, och har anpassats med hänsyn till uppgifternas känslighet, intresset av insyn och intresset av skydd i vissa specifika verksamheter. Det är förbjudet för myndigheter att röja en sekretessbelagd uppgift. Förbudet gäller också för en person som fått kännedom om uppgiften genom att för det allmännas räkning delta i en myndighets verksamhet på grund av anställning eller uppdrag hos myndigheten, på grund av tjänsteplikt eller på annan liknande grund (2 kap. 1 § OSL).

I den privata sektorn gäller i stället som huvudregel att den som disponerar över information i princip själv bestämmer om utlämnande av den till andra, med de begränsningar som dataskyddsregleringen ställer upp. Inom flera olika verksamhetsområden i den privata sektorn gäller emellertid tystnadsplikt enligt lag, ofta reglerad som ett förbud mot att röja vissa uppgifter obehörigen. Det gäller bland annat verksamheter i välfärdssektorn såsom skola och hälso- och sjukvård. Men det finns också exempel på tystnadsplikt i privat verksamhet som inte har någon motsvarighet i det allmännas verksamhet, utan som skyddar information som lämnas till personer i olika slag av förtroendeställning, såsom exempelvis tystnadsplikt för revisorer och skyddsombud, eller den tystnadsplikt som följer av den så kallade banksekretessen.⁸

I dessa fall har obehörighetsrekvisitet sammanfattningsvis tolkats som att ett utlämnande av uppgifter får ske om den uppgiften rör har lämnat sitt samtycke, om uppgifter lämnas vidare till personer inom den berörda verksamheten som behöver dem för verksamheten eller om uppgifterna enligt lag eller annan författning ska lämnas ut, exempelvis till en tillsynsmyndighet.⁹

Författningsreglerad tystnadsplikt, oavsett om den följer av offentlighets- och sekretesslagen eller av särskilda bestämmelser om tystnadsplikt för den privata sektorn, är som regel förenad med straffansvar. I 20 kap. 3 § brottsbalken regleras det generella straffansvaret för brott mot tystnadsplikt. Straffansvaret gäller var och en som har skyldighet att hemlighålla en uppgift enligt lag eller annan författning, förutsatt att straffansvaret inte har reglerats särskilt. Konsekvensen av att en tystnadsplikt införs i författning blir alltså, om inget annat stadgas, att med regleringen följer ett straffansvar.

Vår bedömning

Det finns inget uttalande i skälen som ger ledning vid tolkning av kravet på sekretess för dataskyddsombud i förordningens artikel 38.5. Sannolikt syftar bestämmelsen till att skydda framför allt sådan information om den personuppgiftsansvariges eller biträdets affärs- och

⁸ 9 kap. 41 § aktiebolagslagen (2005:551) och 26 § revisorslagen (2001:883), 7 kap. 13 § arbetsmiljölagen (1977:1160) samt 1 kap. 10 § lagen (2004:297) om bank- och finansieringsrörelse.

⁹ Se exempelvis prop. 2002/03:139 s. 479.

driftsförhållanden som dataskyddsbudet kan komma att få tillgång till vid utövandet av sitt uppdrag. Det kan dock inte uteslutas att avsikten också har varit att skydda anmälares namn eller andra uppgifter om enskildas personliga förhållanden.

Det faktum att bestämmelsen hänvisar till nationell rätt innebär att medlemsstaterna har stor frihet att utforma en lämplig reglering. Eftersom bestämmelsen enligt sin ordalydelse är tvingande finns det däremot enligt vår bedömning ingen möjlighet att helt lämna denna fråga oreglerad.

För det allmännas räkning kan det enligt vår mening inte komma ifråga att särskilt reglera sekretessen för dataskyddsbud, utöver den sekretess som redan gäller i alla de vitt skilda verksamhetstyper som omfattas av dataskyddsförordningens tillämpningsområde. Det får förutsättas att det i verksamheter där känsliga uppgifter förekommer redan gäller sekretess enligt offentlighets- och sekretesslagen i den utsträckning som är motiverad i just den verksamheten. Så länge dataskyddsbudet innehar en sådan anställning eller uppdrag som avses i 2 kap. 1 § andra stycket OSL omfattas han eller hon av sekretessen. Vår bedömning är att ett dataskyddsbud i allmänhet får anses delta i verksamheten på ett sådant sätt som förutsätts i nämnda bestämmelse.

Vi bedömer inte heller att ett dataskyddsbud som innehar en sådan anställning eller ett sådant uppdrag i allmänhet kan anses uppträda självständigt i förhållande till den övriga verksamheten inom myndigheten i den mening som avses i 2 kap. 8 § tryckfrihetsförordningen. På många sätt påminner dataskyddsbudets ställning enligt förordningens artikel 38 om den som en internrevisor intar när det gäller självständighet och förhållande till ledningen.¹⁰ Högsta förvaltningsdomstolen har i HFD 2013 ref. 40 bedömt att en internrevisor vid Jordbruksverket inte intog en sådan självständig ställning att en rapport som överlämnats till den granskade verksamheten skulle anses expedierad.

Om det skulle visa sig att tystnadsplikten för dataskyddsbud i det allmännas verksamhet är otillräcklig, får frågan om en särskild sekretessreglering övervägas på nytt.

¹⁰ En internrevisor vid en myndighet ska enligt internrevisionsförordningen (2006:1228) och Ekonomistyrningsverkets tillhörande föreskrifter, ESV Cirkulär 2007:1, senast ändrade genom ESV Cirkulär 2015:4, inrättas direkt under myndighetens ledning och vara självständig i förhållande till den granskade verksamheten.

Utanför den krets som anges i 2 kap. 2–4 §§ OSL – dvs. myndigheter, sådana juridiska personer där kommuner och landsting har ett rättsligt bestämmande inflytande och de organ som finns upptagna i bilagan till offentlighets- och sekretesslagen – finns det däremot ingen reglering som skyddar uppgifter som dataskyddsombudet får tillgång till vid utförandet av sitt uppdrag. För att Sverige ska uppfylla dataskyddsförordningens krav måste bestämmelser om tystnadsplikt för dataskyddsombud i den privata sektorn införas.

Som framgår ovan finns det en rad tystnadsplikter som är ägnade att skydda uppgifter som lämnas till personer som i egenskap av sin ställning och för att kunna utföra sitt uppdrag måste åtnjuta förtroende, såsom exempelvis revisorer och skyddsombud. Dataskyddsombudets ställning kan i vissa avseenden likställas med revisorns eller skyddsombudets, och tystnadsplikten för dataskyddsombud bör därför utformas på ett liknande sätt. Tystnadsplikten ska således avgränsas med ett obehörighetsrekvisit vilket bland annat innebär att uppgifter kan lämnas ut med samtycke, till tillsynsmyndighet eller annars som en följd av en skyldighet i lag eller författning.

17.5 Sekretess för uppgifter som behandlas i strid mot personuppgiftsregleringen

17.5.1 Gällande rätt

Sekretessbestämmelsen i 21 kap. 7 § OSL innebär att sekretess gäller för personuppgifter, om det kan antas att ett utlämnande skulle medföra att uppgiften behandlas i strid med personuppgiftslagen. Även om paragrafens formulering är något oklar, får det numera anses fastslaget i praxis att den enbart tar sikte på mottagarens behandling av personuppgifter.¹¹ Det som ska bedömas enligt bestämmelsen är alltså endast huruvida mottagarens avsedda behandling av de personuppgifter som begärs ut uppfyller kraven enligt personuppgiftslagen.

Sekretessen enligt 21 kap. 7 § OSL gäller med ett rakt skaderekvisit, dvs. det ska presumeras att sekretess inte hindrar att personuppgifterna lämnas ut. I förarbetena till den motsvarande sekretessbestämmelse som gällde under datalagens tid anfördes att en begäran

¹¹ HFD 2014 ref. 66.

om massuttag eller selekterade uppgifter alltid borde utgöra anledning för myndigheten att närmare utreda hur det är avsett att uppgifterna ska användas och att det är först om sökanden kan ange en godtagbar förklaring som uppgifterna bör lämnas ut.¹²

Bestämmelsen i 21 kap. 7 § OSL har utretts flera gånger under 2000-talet. Inledningsvis sågs den över av Offentlighets- och sekretesskommittén (SOU 2003:99) och därefter av Personuppgiftslagsutredningen (SOU 2004:6). Personuppgiftslagsutredningen föreslog bland annat att det skulle förtydligas att prövningen enligt sekretessbestämmelsen ska avse om det kan antas att uppgifterna efter ett utlämnande kommer att behandlas i strid med personuppgiftslagen. Riksdagens ombudsmän (JO) har i remissyttranden över dessa betänkanden anfört att sekretessbestämmelsen bör upphävas. Som skäl har JO bland annat anfört att en sekretessbestämmelse som förutsätter att en myndighet måste skaffa sig en uppfattning om syftet med en begäran om utlämnande av handlingar eller uppgifter stämmer dåligt med det s.k. efterfrågeförbudet i 2 kap. 14 § tredje stycket tryckfrihetsförordningen.¹³ Varken Offentlighets- och sekretesskommitténs eller Personuppgiftslagsutredningens förslag till ändring av sekretessbestämmelsen har genomförts.

Frågan om tillämpningen av 21 kap. 7 § OSL har också utförligt behandlats av E-offentlighetskommittén, som bland annat hade till uppgift att överväga om bestämmelsen borde upphävas. Kommittén fann att bestämmelsen fyller i vart fall en viss begränsad funktion och därför inte borde upphävas. Vidare föreslog kommittén bland annat att bestämmelsen skulle förtydligas så att det inte råder någon tvekan om att det bara är sökandens efterföljande behandling som är relevant för den sekretessprövning som ska göras och inget annat.¹⁴ Förslaget har ännu inte lett till lagstiftning. Bestämmelsens innebörd och historik behandlas också utförligt i Informationshanteringsutredningens betänkande.¹⁵

JO har uttalat följande till klargörande av hur bestämmelsen ska tillämpas mot bakgrund av efterfrågeförbudet i 2 kap. 14 § tredje stycket tryckfrihetsförordningen (dnr 1102-2004).

¹² Prop. 1973:33 s. 140.

¹³ JO dnr 1102-2004 och 1849-2004.

¹⁴ SOU 2010:4 s. 317 f.

¹⁵ SOU 2015:39 s. 436 f.

Det står klart att myndigheten inte får börja ställa frågor om sökandens tilltänkta användning bara för att en personuppgift begärs utlämnad. Det krävs för det första att det finns någon konkret omständighet som gör att det kan antas att personuppgiften efter utlämnandet kommer att behandlas på ett sätt som omfattas av personuppgiftslagen. Sådana omständigheter kan – förutom de upplysningar som sökanden på eget initiativ kan ha lämnat om sin tilltänkta användning av uppgifterna – vara att sökanden begär att få ut uppgifter om väldigt många personer från ett register (ett s.k. massuttag) eller uppgifter om ett urval av personer med vissa karakteristika, t.ex. inkomst, språktillhörighet, politisk tillhörighet osv. (s.k. selekterade uppgifter). Först om det på grund av någon konkret omständighet finns skäl att anta att sökanden kommer att behandla uppgifterna på ett sätt som omfattas av personuppgiftslagen, t.ex. därför att begäran omfattar uppgifter om många personer, finns det anledning att genom frågor till sökanden försöka ta reda på hur och till vad sökanden ska använda uppgifterna för att kunna bedöma om den tilltänkta behandlingen strider mot personuppgiftslagen. Myndigheten får dock enligt 2 kap. 14 § tredje stycket tryckfrihetsförordningen inte ställa mer inträngande eller fler frågor än som behövs för att göra en sekretessbedömning.

Det är vidare värt att notera att det i praxis har tydliggjorts att sekretessen inte gäller om de utlämnade uppgifterna ska behandlas av personuppgiftsansvariga som är etablerade utomlands, där personuppgiftslagen inte är tillämplig (HFD 2014 ref. 66).

17.5.2 Överväganden och förslag

Utredningens förslag: Sekretess ska gälla för personuppgift, om det kan antas att uppgiften efter ett utlämnande kommer att behandlas i strid med dataskyddsförordningen eller dataskyddslagen.

Bestämmelsen i 21 kap. 7 § OSL har som framgått ovan varit föremål för överväganden under lång tid. Den senaste utvärderingen, som skedde av den parlamentariskt sammansatta E-offentlighetskommittén, kom fram till att bestämmelsen fortsatt fyller en viss begränsad funktion och inte bör upphävas. Våra direktiv lämnar inte utrymme för överväganden som rör ett eventuellt upphävande av bestämmelsen, utan handlar enbart om anpassning av bestämmelsen till den nya regleringen. Det kan dock i detta sammanhang konstateras att

det följer av förordningens artikel 86 att nationella bestämmelser om tillgång till allmänna handlingar ges företräde framför förordningens bestämmelser om skydd för personuppgifter. I artikeln nämns att detta görs för att jämka samman allmänhetens rätt att få tillgång till handlingar med rätten till skydd av personuppgifter enligt förordningen. Bestämmelsen i 21 kap. 7 § OSL innebär ett uttryckligt stöd i svensk rätt för en sådan sammanjämkning mellan de nämnda rättigheterna, vilket möjligen ytterligare talar för att bestämmelsen fyller en funktion även fortsättningsvis.

Eftersom vi föreslår att personuppgiftslagen ska upphävas och materiellt ersättas av dataskyddsförordningen och vårt förslag till dataskyddslag, måste bestämmelsen ändras.

Den lösning som ligger närmast till hands är enligt vår mening då att ersätta hänvisningen till personuppgiftslagen med en hänvisning till dataskyddsförordningen och den dataskyddslag vi föreslår. Detta kan innebära en risk för att den prövning som ska utföras kompliceras något. Förordningens bestämmelser är betydligt mer omfattande och i vissa avseenden mer detaljerade än personuppgiftslagens. Det bör dock betonas att det som en utlämnande myndighet ska pröva är om det *kan antas* att en uppgift efter ett utlämnande kommer att behandlas i strid med förordningen eller dataskyddslagen. Som framgår av äldre förarbeten och JO:s uttalanden får vidare undersökningar vidtas endast om det finns konkreta omständigheter som indikerar att mottagaren kommer att behandla uppgifterna på ett sätt som strider mot dataskyddsregleringen, t.ex. massuttag eller selekterade uttag. Finns det inga sådana indikationer behöver inte någon bedömning enligt dataskyddsregleringen göras. Rekviritet "kan antas" torde också innebära att någon fullständig bedömning av om behandlingen kommer att strida mot förordningen inte krävs.

En materiell skillnad som den föreslagna förändringen kommer att medföra är att utlämnanden till utländska mottagare som omfattas av dataskyddsförordningens tillämpningsområde också kommer att omfattas av sekretessbestämmelsen.

Vår bedömning är att den ordning som tydliggjorts genom Högsta förvaltningsdomstolens avgörande (HFD 2014 ref. 66) innebär en omotiverad åtskillnad i skydd för personuppgifter som lämnas ut till personuppgiftsansvariga som inte är etablerade i Sverige. Det medför att svenska personuppgiftsansvariga missgynnas jämfört med personuppgiftsansvariga i andra medlemsstater på ett sätt som kan

ifrågasättas utifrån dataskyddsförordningens syfte. En ordning där bestämmelsen inte är tillämplig gentemot personuppgiftsansvariga som är etablerade i andra medlemsstater innebär också att bestämmelsen lätt kan kringgås genom att uppgifter begärs utlämnade av en sådan personuppgiftsansvarig för en svensk personuppgiftsansvarigs räkning. Mot bakgrund av ovanstående anser vi att denna materiella utvidgning av bestämmelsens tillämpningsområde är rimlig och ligger väl i linje med de grundläggande principerna i dataskyddsförordningen.

Det är numera klarlagt att prövningen av 21 kap. 7 § OSL gäller den behandling som kommer att ske efter ett eventuellt utlämnande. E-offentlighetskommitténs förslag för att förtydliga detta i lagtext har inte mött någon kritik från remissinstanserna. Vi föreslår därför att lagtexten ska justeras så att det tydligt framgår att det är behandling efter ett utlämnande som avses.

Eftersom den här föreslagna hänvisningen avser dataskyddsförordningen i dess helhet och innebär en tydlig inskränkning i den grundlagsstadgade handlingsoffentligheten, bör hänvisningen vara statisk, dvs. avse den ursprungliga lydelsen av förordningen. Det medför att lagstiftaren aktivt måste bedöma om eventuella ändringar och tillägg till förordningen ska omfattas av 21 kap. 7 § OSL.

17.6 Generalklausulen

17.6.1 Gällande rätt

Den så kallade generalklausulen i 10 kap. 27 § OSL möjliggör utlämnande av uppgifter som omfattas av sekretess mellan myndigheter även i fall då det saknas uttryckliga sekretessbrytande regler. Utlämnandet ska då prövas enligt den intresseavvägning och med beaktande av det uppenbarhetsrekvisit som framgår av bestämmelsen. Av paragrafens andra stycke framgår att viss sekretess, som hälso- och sjukvårdssekretessen och socialtjänstsekretessen, undantas från tillämpningsområdet.

I tredje stycket samma paragraf undantas också utlämnanden som strider mot lag eller förordning eller föreskrift som har meddelats med stöd av personuppgiftslagen från tillämpningsområdet. Första ledet har ansetts innebära att en förutsättning för att generalklausulen ska vara tillämplig är att utlämnandet inte strider mot en sådan

specialreglering av uppgiftslämnandet i fråga som finns i lag eller förordning. Om det t.ex. i lag har föreskrivits att en viss myndighet för sin verksamhet på angivna villkor kan få ta del av även hemliga uppgifter hos en annan myndighet, kommer det inte i fråga att, när de angivna villkoren inte är uppfyllda, lämna ut uppgifterna med stöd av generalklausulen i stället.¹⁶

Innebörden av tredje styckets andra led är numera oklar. Tidigare avsåg den en möjlighet för Datainspektionen att meddela vissa villkor om utlämnande för vissa register i samband med tillståndsgivning. I kommentaren till den numera upphävda sekretesslagen (1980:100) har det ansetts att det efter datalagens upphörande och införandet av personuppgiftslagen är reglerna i själva personuppgiftslagen och inte föreskrifter i enskilda beslut av Datainspektionen som får betydelse för behandlingen av generalklausulen.¹⁷

17.6.2 Överväganden och förslag

Utredningens förslag: Hänvisningen till personuppgiftslagen i generalklausulen ska strykas. Generalklausulen ska enligt den nya lydelsen inte tillämpas om utlämnandet strider mot lag eller förordning.

Det finns ingen praxis som tydliggör innebörden av hänvisningen till personuppgiftslagen i 10 kap. 27 § tredje stycket andra ledet OSL och innebörden har som redogjorts för ovan ansetts oklar och bestämmelsen tycks inte längre fylla någon praktisk funktion.

Det första ledet i generalklausulens tredje stycke innebär enligt sin ordalydelse att ett utlämnande till annan myndighet med stöd av generalklausulen inte får ske om det skulle strida mot lag eller förordning, exempelvis mot personuppgiftslagen. En hänvisning till lag i offentlighets- och sekretesslagen innefattar också EU-förordningar.¹⁸ Redan det första ledet torde alltså innebära att ett utlämnande till annan myndighet som strider mot dataskyddsförordningen eller data-

¹⁶ Prop. 1979/80:2, del A s. 328.

¹⁷ Lenberg m.fl., Offentlighets- och sekretesslagen (8 november 2016, Zeteo), kommentaren till 10 kap. 27 § OSL, och Regner m.fl., Sekretesslagen (1 april 2009, Zeteo), kommentaren till 14 kap. 3 § sekretesslagen.

¹⁸ Prop. 1998/99:18 s. 41 och 75 samt prop. 1999/2000:126 s. 160 och 283.

skyddslagen inte kan ske med stöd av generalklausulen. Någon mot- svarighet till andra ledet i tredje stycket behövs enligt vår bedömning inte som en följd av den nya regleringen. Vi föreslår därför att det andra ledet stryks.

17.7 Sekretess för uppgifter i verksamhet för teknisk bearbetning och lagring

17.7.1 Gällande rätt

Sekretessen enligt 40 kap. 5 § OSL gäller i en myndighets verksamhet som består av enbart teknisk bearbetning eller teknisk lagring för någon annans räkning av sådana personuppgifter som avses i personuppgiftslagen. Sekretessen gäller hos en myndighet som behandlar personuppgifter såväl då det är fråga om bearbetning eller lagring för enskildas räkning som då det gäller bearbetning eller lagring av en annan myndighets personuppgifter. Med teknisk bearbetning avses t.ex. att myndigheten scannar in text på papper för att lagra elektroniskt. Teknisk lagring avser alla former av lagring som kräver särskilda tekniska anordningar, t.ex. lagring av information på hårddisk eller i molntjänster. Personuppgifter som förvaras hos en arkivmyndighet anses normalt inte tekniskt lagrade för någon annans räkning.¹⁹

Sekretessens räckvidd är avgränsad till verksamhet avseende personuppgifter som avses i personuppgiftslagen, dvs. enligt den definition som finns i 3 § PUL. Sekretessens föremål, dvs. de uppgifter som skyddas av bestämmelsen, är uppgifter om enskildas personliga och ekonomiska förhållanden. Detta omfattar inte bara personuppgifter utan även exempelvis uppgifter om juridiska personer. Sekretessen är som nämnts absolut.

Tryckfrihetsförordningens reglering i 2 kap. 10 § första stycket innebär att handlingar som förvaras hos en myndighet endast som ett led i teknisk bearbetning eller lagring inte är att anse som allmänna handlingar där. Det innebär i sin tur att bestämmelsen i 40 kap. 5 § OSL inte har någon praktisk betydelse för utlämnande av uppgifter i allmänna handlingar, utan endast fyller funktionen av en tyst-

¹⁹ Lenberg m.fl., Offentlighets- och sekretesslagen (8 november 2016, Zeteo), kommentaren till 40 kap. 5 § OSL.

nadspliktsbestämmelse som hindrar utlämnande på myndighetens eller befattningshavarens eget initiativ.

17.7.2 Överväganden och förslag

Utredningens förslag: Sekretess ska gälla för uppgift om en enskilds personliga eller ekonomiska förhållanden i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning av sådana personuppgifter som avses i dataskyddsförordningen.

Tillämpningsområdet för sekretessbestämmelsen i 40 kap. 5 § OSL är begränsat till teknisk bearbetning eller lagring av personuppgifter enligt personuppgiftslagens definition. Personuppgifter definieras i 3 § PUL som ”all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet”. Eftersom personuppgiftslagen ska upphävas enligt vårt förslag måste bestämmelsen anpassas.

För att anpassa bestämmelsen till den nya regleringen ligger det nära till hands att ersätta hänvisningen till personuppgiftslagen med en hänvisning till dataskyddsförordningens definition av personuppgifter. Den överensstämmer i stora drag med personuppgiftslagen, även om den är mer detaljerad. Definitionen i artikel 4.1 lyder som följer.

Varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Av förordningens skäl 27 framgår att förordningen inte gäller behandling av personuppgifter rörande avlidna personer. Sammantaget bedömer vi att förordningens definition inte är tydligt vidare än den som finns i dag i personuppgiftslagen. Kopplingen mellan sekretessbestämmelsen och den definition av personuppgifter som återfinns i dataskyddsregleringen har funnits sedan paragrafen infördes i

dåvarande sekretesslagen och vi ser ingen anledning att ändra på den ordningen. Hänvisningen till personuppgiftslagens definition av personuppgifter bör därför ersättas med en hänvisning till personuppgiftsbegreppet i den betydelse det har i dataskyddsförordningens artikel 4.1. Eftersom hänvisningen i praktiken inte begränsar handlingsoffentligheten och bara avser själva definitionen av personuppgifter bör den vara dynamisk, dvs. avse den vid varje tidpunkt gällande definitionen i förordningen.

18 Sanktioner

18.1 Vårt uppdrag

Vårt uppdrag när det gäller sanktioner består av flera delar. Vi ska analysera om, och i så fall i vilken utsträckning, det bör vara möjligt att besluta om administrativa sanktionsavgifter inom den offentliga sektorn. En jämförelse ska göras med vad som gäller för t.ex. viten i allmänhet, miljöstraffavgifter och sanktionsavgifter på arbetsmiljöområdet.

Vi ska analysera och ta ställning till i vilken utsträckning överträdelser av förordningen bör bli föremål för ytterligare sanktioner, vid sidan om de sanktionsavgifter som föreskrivs i förordningen. Vi ska också analysera om, och i så fall i vilken utsträckning, dessa sanktioner bör vara tillämpliga inom den offentliga sektorn.

Slutligen ska vi analysera hur en reglering med både administrativa sanktionsavgifter och andra sanktioner förhåller sig till det s.k. dubbelprövningsförbudet i artikel 4.1 i Europakonventionens sjunde tilläggsprotokoll och artikel 50 i EU:s stadga om de grundläggande rättigheterna.

18.2 Vad är en sanktion?

Det finns ingen legaldefinition av begreppet sanktion. Klart är att en sanktion alltid har ett handlingsdirigerande eller bestraffande syfte. En vid definition skulle kunna omfatta alla former av påföljder som kan följa på ett rättsstridigt handlande.

Det är enligt vår mening av vikt att presentera en samlad bild av de konsekvenser överträdelser av personuppgiftsregleringen kan få enligt gällande rätt och enligt dataskyddsförordningen, för att mot den bakgrunden kunna göra de bedömningar som ingår i vårt upp-

drag. I detta avsnitt behandlas därför sanktioner i vid mening, inbegripet regleringen om straff, sanktionsavgifter, vite och skadestånd.

18.3 Gällande rätt

18.3.1 Skadestånd

Enligt dataskyddsdirektivets artikel 23 ska medlemsstaterna föreskriva att den som har lidit skada genom otillåten behandling eller någon annan åtgärd som är oförenlig med de nationella bestämmelser som antagits till följd av direktivet har rätt till ersättning av den personuppgiftsansvarige för skadan.

Artikeln har genomförts i svensk rätt genom 48 § PUL, där det stadgas att den personuppgiftsansvarige ska ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling i strid med lagen har orsakat. Ersättningsskyldigheten kan enligt paragrafens andra stycke jämkas om den personuppgiftsansvarige visar att felet inte beror på honom eller henne. Ersättning kan utgå såväl för ekonomisk som ideell skada (kränkning). Ansvar är strikt och det krävs alltså inte att den personuppgiftsansvarige eller någon annan har haft uppsåt att handla i strid med lagen eller varit oaktsam. Skadeståndsregleringen i personuppgiftslagen får anses strängare än vad som krävs enligt dataskyddsdirektivet och har bedömts innebära en effektiv sanktion mot överträdelser av regleringen.¹ Det bör noteras att bestämmelsen endast gäller behandling i strid med personuppgiftslagen, och alltså inte direkt gäller behandling i strid med sektorslagstiftning. Många sektorsspecifika författningar innehåller emellertid en hänvisning till skadeståndsbestämmelsen i personuppgiftslagen.

Justitiekanslern har möjlighet att på frivillig väg reglera vissa skadeståndsanspråk som riktas mot staten, bland annat enligt skadeståndsregleringen i personuppgiftslagen. Tanken med det är att avlasta domstolarna uppgiften att pröva mål där det egentligen inte finns någon tvist, utan där det är klart att ett skadeståndsgrundande fel har begåtts och att den enskilde har rätt till viss ersättning (2 a § förordningen [1975:1345] med instruktion för Justitiekanslern, samt

¹ Öman och Lindblom, Personuppgiftslagen (20 december 2016, Zeteco), kommentaren till rubriken Skadestånd i personuppgiftslagen.

förordningen [1995:1301] om handläggning av skadeståndsanspråk mot staten).

En genomgång av Justitiekanslerns praxis angående skadeståndsanspråk mot staten med anledning av 48 § PUL finns i Informationshanteringsutredningens betänkande, SOU 2015:39 s. 643 f. Som exempel på skador på grund av överträdelse av personuppgiftslagen som enligt Justitiekanslerns beslut medfört ersättningskyldighet kan nämnas bristande gallringsrutiner och felaktiga personuppgifter i olika register, exempelvis i folkbokföringsdatabasen och i socialförsäkringsdatabasen. Värt att nämna särskilt i detta sammanhang är Justitiekanslerns beslut den 7 maj 2014 (dnr 1441-14-47) där skadeståndsanspråket rörde registrering av personuppgifter i det s.k. Kringresanderegistret i strid med polisdatalagen (2010:361). Polisdatalagen hänvisar till skadeståndsbestämmelsen i personuppgiftslagen. Omkring 3 000 personer ansökte om skadestånd hos Justitiekanslern för registrering. Justitiekanslern ansåg att de registrerade var berättigade till en ersättning om 5 000 kronor per registrerad person.²

18.3.2 Straff

Dataskyddsdirektivet överlåter enligt artikel 24 till medlemsstaterna att besluta om de sanktioner som ska användas vid överträdelse av bestämmelserna om behandling av personuppgifter. Med stöd av artikeln infördes 49 § PUL. Paragrafen innehåller en straffbestämmelse avseende brott mot vissa bestämmelser i lagen, bland annat om man lämnar osann uppgift i information till registrerade eller till tillsynsmyndigheten, behandlar känsliga personuppgifter i strid med personuppgiftslagen eller för över personuppgifter till tredje land utan att beakta kravet på adekvat skydds nivå. För straffbarhet krävs det uppsåt eller grov oaktsamhet. Det är den fysiska person som har gjort sig skyldig till förfarandet eller underlåtenheten som döms till straff oavsett om han eller hon själv är personuppgiftsansvarig. För ringa fall döms inte till ansvar. Den som överträtt ett vitesförelägg-

² Stockholms tingsrätt har efter att elva av de registrerade ansökt om stämning mot staten, tillerkänt dem ytterligare ersättning om 30 000 kr var, se Stockholms tingsrätts dom den 10 juni 2016 i mål nr T 2978-15, T 2986-15, T 2993-15, T 2996-15, T 2998-15, T 3002-15, T 3006-15, T 3010-15, T 3011-15, T 3012-15 och T 3013-15. Svea hovrätt har fastställt tingsrättens dom, se hovrättens dom den 28 april 2017 i mål nr T 6161-16.

gande döms inte heller till ansvar för samma gärning som vitesföreläggandet avser.

De mål som har prövats enligt straffbestämmelsen har framför allt handlat om publiceringar på internet och de flesta är av äldre datum – innan EU-domstolen klargjorde att publiceringar på internet inte innebär en överföring av personuppgifter till tredje land.³ Straffbestämmelsen har sällan använts på senare år, bland annat eftersom det har funnits svårigheter med att lagföra kränkningar på internet med stöd av bestämmelsen. Lagstiftningen uppfattas som komplicerad och det grundlagsskyddade området begränsar det straffbara området väsentligt.⁴

Vid sidan av straffbestämmelsen i personuppgiftslagen finns andra straffbestämmelser som också kan innebära att vissa gärningar som innefattar personuppgiftsbehandling omfattas av straffansvar – såsom bestämmelserna om dataintrång (4 kap. 9c § brottsbalken), kränkande fotografering (4 kap. 6a § brottsbalken), förtal (5 kap. 1 § brottsbalken) och tjänstefel (20 kap. 1 § brottsbalken). För en utförlig genomgång av det straffrättsliga integritetsskyddet i brottsbalken, se SOU 2016:7 s. 208 f.

18.3.3 Vite

Enligt 44 och 45 §§ PUL får Datainspektionen vid vite förbjuda en personuppgiftsansvarig att fortsätta att behandla uppgifter på annat sätt än att lagra dem, om inspektionen inte på begäran får tillgång till ett tillräckligt underlag för att konstatera att behandlingen är laglig eller om tillsynsmyndigheten konstaterar att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt. Detsamma gäller om den personuppgiftsansvarige inte frivilligt följer ett beslut om säkerhetsåtgärder. Bestämmelserna om vite gäller även för statliga och kommunala myndigheter som är personuppgiftsansvariga. I praktiken har dock Datainspektionen aldrig utnyttjat möjligheten att vitesförelägga.

Några uttryckliga bestämmelser om vite finns inte i dataskyddsdirektivet. Det kan noteras att Datalagskommittén ansåg att vites-

³ Dom Lindqvist, C-101/01, EU:C:2003:596, punkt 70.

⁴ SOU 2016:7 s. 273 f., Svahn Starrsjö, Personuppgiftslagen och yttrandefriheten, SvJT 100 år (jubileumsskrift) s. 447.

förelägganden – och utdömandet av förelagda vite – utgör sådana särskilda sanktioner som medlemsstaterna ska besluta om enligt dataskyddsdirektivets artikel 24.⁵

I sektorsspecifika författningar finns bestämmelser som innebär en inskränkning i Datainspektionens möjligheter att förelägga vite.⁶ Skälen för dessa inskränkningar i Datainspektionens befogenheter varierar. I vissa fall är argumentet att vite som sanktionsmedel enligt allmänna rättsgrundsatser inte bör användas mellan statliga myndigheter.⁷

18.4 Dataskyddsförordningen

18.4.1 Skadestånd

Enligt förordningens artikel 82.1 ska varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av förordningen ha rätt till ersättning från den personuppgiftsansvarige för den uppkomna skadan. En nyhet i förordningen är att även personuppgiftsbiträden kan bli skadeståndsskyldiga under vissa förutsättningar. I skäl 146 och artikel 82.2–5 preciseras närmare under vilka förutsättningar personuppgiftsansvariga och personuppgiftsbiträden kan hållas ansvariga för uppkomna skador. Bland annat anges där att varje personuppgiftsansvarig eller personuppgiftsbiträde som medverkat vid behandlingen ska ansvara för uppkommen skada. Det stadgas också att den personuppgiftsansvarige eller personuppgiftsbiträdet ska undgå ansvar om de visar att de inte på något sätt är ansvariga för den händelse som orsakade skadan. Sammantaget leder detta tanken till att ett i princip strikt skadeståndsansvar gäller enligt förordningen för såväl ekonomisk som ideell skada, dvs. en liknande reglering som den som gäller enligt personuppgiftslagen. Den närmare innebörden av bestämmelserna får dock utvecklas i rättspraxis.

Förordningen innebär också ett förtydligande jämfört med direktivet på så sätt att varje personuppgiftsansvarig eller personuppgifts-

⁵ SOU 1997:39 s. 437 f.

⁶ Så är fallet i exempelvis 1 kap. 3 § lagen (2001:181) om behandling av personuppgifter i Skatteverkets beskattningsverksamhet, i 1 kap. 3 § lagen (2001:183) om behandling av personuppgifter i verksamhet med val och folkomröstningar och i 1 kap. 3 § lagen (2001:184) om behandling av personuppgifter i Kronofogdemyndighetens verksamhet.

⁷ Prop. 2000/01:33 s. 96, prop. 2004/05:164 s. 54 och prop. 2009/10:85 s. 90.

biträde som har medverkat vid en behandling kan hållas ansvarig för hela skadan, dvs. att ett solidariskt ansvar gäller när det finns flera personuppgiftsansvariga eller personuppgiftsbiträden som är ansvariga för samma behandling.

18.4.2 Administrativa sanktionsavgifter

Administrativa sanktionsavgifter är en nyhet i dataskyddsförordningen som inte finns med i dataskyddsdirektivet eller den nuvarande svenska personuppgiftsregleringen. Sanktionsavgifterna införs enligt skäl 148 för att stärka verkställigheten av förordningen.

Bestämmelserna om administrativa sanktionsavgifter återfinns i förordningens i artikel 83 och förtydligas i skäl 148–150. Av artikel 83.1 framgår att det är den nationella tillsynsmyndigheten som ska besluta om sanktionsavgifter vid överträdelser av förordningens bestämmelser. I artikel 83.2 finns en detaljerad reglering av vilka faktorer som ska beaktas vid beslut om sanktionsavgifter och bestämmande av avgiftens storlek. Bland annat ska tillsynsmyndigheten vid beslutet beakta överträdelsens karaktär, svårighetsgrad och varaktighet, samt om överträdelsen skett med uppsåt eller genom oaktsamhet. Det är alltså inte ett uttryckligt krav i förordningstexten att överträdelsen ska ha skett med uppsåt eller oaktsamhet för att sanktionsavgift ska bli aktuellt, men subjektiva omständigheter hos den personuppgiftsansvarige är en faktor som ska beaktas.

Andra faktorer som tillsynsmyndigheten ska beakta är antalet berörda registrerade, vilken skada de har lidit, om den personuppgiftsansvarige har försökt förebygga eller i efterhand komma till rätta med överträdelsen och eventuell ekonomisk vinst som görs, eller ekonomisk förlust som undviks, genom överträdelsen. Av skälen framgår vidare att avsikten har varit en viss flexibilitet när en sanktionsavgift beslutas mot en fysisk person. I skäl 148 anges till exempel att om en sanktionsavgift som ”sannolikt skulle utdömas” skulle innebära en oproportionell börda för en fysisk person får en reprimand utfärdas i stället. I skäl 150 anges också att den allmänna inkomstnivån i medlemsstaten och personens ekonomiska situation bör beaktas när sanktionsavgiften fastställs mot en fysisk person. Förordningens bestämmelser tycks alltså ge utrymme för att beakta uppsåt, proportionalitet och betalningsförmåga vid beslut om sank-

tionsavgifterna, vilket inte alltid är fallet när det gäller sanktionsavgifter på andra områden.⁸

I artikel 83.3 stadgas att om flera överträdelser görs får avgiftens totala belopp inte överstiga det belopp som fastställs för den allvarligaste överträdelsen. I artikel 83.4 och 83.5 fastställs övre beloppsgränser för de två olika kategorier av överträdelser som kan föranleda sanktionsavgifter enligt förordningen. För de något mindre allvarligare överträdelserna, såsom överträdelser av regler om inbyggt data-skydd, förteckningar och konsekvensbeskrivningar, fastslås ett maxbelopp på 10 000 000 EUR eller 2 procent av den globala årsomsättningen om det gäller ett företag, beroende på vilket belopp som är högst. För allvarligare överträdelser, såsom överträdelser av regler om de grundläggande principerna för behandling och behandling av känsliga personuppgifter, registrerades rätt till information, rättelse och radering, överföring av uppgifter till tredje land och underlåtenhet att rätta sig efter tillsynsmyndighetens förelägganden, fastslås ett maxbelopp om 20 000 000 EUR eller 4 procent av den globala årsomsättningen.

Det stora flertalet bestämmelser i förordningen som innehåller rättigheter eller skyldigheter för personuppgiftsansvariga, personuppgiftsbiträden samt eventuella certifieringsorgan och övervakningsorgan omfattas av regleringen om sanktionsavgifter, vilket framgår av hänvisningar i artikel 83.4–6. För samtliga de artiklar som artikel 83 hänvisar till ska alltså en överträdelse föranleda att sanktionsavgift påförs, om förutsättningarna i övrigt är uppfyllda enligt artikel 83.2.

I allmänhet är de bestämmelser i förordningen som inte nämns i artikel 83 sådana som inte innehåller några rättigheter och skyldigheter för enskilda, myndigheter eller andra organ vid sidan av tillsynsmyndigheten och kommissionen. Artikel 10, om behandling av personuppgifter som rör fällande domar i brottmål och andra lagöverträdelser, tillhör emellertid inte denna kategori. Artikel 10 nämns inte i artikel 83.4–6 och omfattas alltså inte av regleringen om sanktionsavgifter. Inga särskilda skrivningar om anledningen till detta finns i skälen eller annars i förordningstexten. Värt att notera är att i kommissionens ursprungliga förslag fanns bestämmelsen om domar i brottmål och andra lagöverträdelser i artikel 9 tillsammans med regle-

⁸ Waring-Nerep Sanktionsavgifter, särskilt i näringsverksamhet s. 209 f., och SOU 2013:38 s. 544 f.

ringen om känsliga personuppgifter, och omfattades därmed av regleringen om sanktionsavgifter. Det kan inte uteslutas att det faktum att artikel 83 inte nämner artikel 10 helt enkelt är en oavsiktlig konsekvens av att bestämmelsen om domar i brottmål och andra överträdelse kom att placeras i en egen artikel i den slutliga versionen av förordningstexten.

Artikel 83.4–6 innehåller inte enbart en uppräkningslista av vilka överträdelse som i sig kan föranleda att sanktionsavgift påförs, utan också bestämmelser om att sanktionsavgifter kan påföras vid olika slag av underlåtenhet att rätta sig efter tillsynsmyndighetens instruktioner, förelägganden eller beslut (artikel 83.5 e och 83.6).

Enligt artikel 83.5 e kan en personuppgiftsansvarig eller ett personuppgiftsbiträde påföras sanktionsavgift vid

- underlåtenhet att rätta sig efter ett föreläggande från tillsynsmyndigheten,
- underlåtenhet att rätta sig efter ett beslut om en tillfällig eller permanent begränsning av behandling av uppgifter,
- underlåtenhet att rätta sig efter ett beslut om att avbryta uppgiftsflöden, eller
- underlåtenhet att ge tillsynsmyndigheten tillgång till uppgifter.

Sanktionsavgiften fyller därmed en vitesliknande funktion.

Vid överträdelse av tillsynsmyndighetens instruktioner, förelägganden och beslut enligt ovan gäller att sanktionsavgift får påföras med det högre maxbeloppet, dvs. 20 000 000 EUR eller 4 procent av den globala årsomsättningen. När det gäller förelägganden från tillsynsmyndigheten upprepas bestämmelsen i artikel 83.6.

Enligt artikel 83.7 får varje medlemsstat reglera om och i vilken utsträckning det ska vara möjligt att besluta om sanktionsavgifter mot offentliga myndigheter och organ i den medlemsstaten.

Artikel 83.8 uppställer krav på effektiva rättsmedel och rättsäkerhet vid beslut om sanktionsavgifter och artikel 83.9 slår fast att om det inte finns några regler om administrativa sanktionsavgifter i en medlemsstats rättssystem får förfarandet inledas av tillsynsmyndigheten och avgiften utdömas av nationell domstol.

Avslutningsvis kan noteras att förordningen inte säger något uttryckligen om vem sanktionsavgifterna ska tillfalla, dvs. om de ska

tillfalla den medlemsstat där den beslutats eller något organ på EU-nivå.

18.4.3 Andra sanktioner

Enligt artikel 84 i förordningen ska medlemsstaterna fastställa regler om andra sanktioner för överträdelse av förordningen, särskilt för sådana som inte är föremål för administrativa sanktionsavgifter. Sanktionerna ska enligt artikeln vara effektiva, proportionella och avskräckande. I skäl 152 anges att medlemsstaterna bör genomföra ett system med effektiva, proportionella och avskräckande sanktioner om förordningen inte harmoniserar administrativa sanktioner eller om det är nödvändigt i andra fall. Det anges också i nämnda skäl att det ska fastställas om sanktionerna ska vara av straffrättslig eller administrativ art.

I skäl 149 anges att medlemsstaterna bör kunna fastställa bestämmelser om straffrättsliga påföljder och möjligheter att förverka den vinning som gjorts vid överträdelse av förordningen. Där erinras också om att utdömandet av sådana påföljder och administrativa sanktioner inte bör medföra ett åsidosättande av dubbelprövningsförbudet enligt EU-domstolens tolkning.

18.5 Sanktionsavgifter inom offentlig sektor

18.5.1 Vad är en sanktionsavgift?

En sanktionsavgift har definierats som en som avgift benämnd penningpåлага som i realiteten utgör en sanktion. Tre kriterier ska enligt doktrinen vara uppfyllda för att något ska kvalificera som en sanktionsavgift. Avgiften ska

1. vara en ekonomisk sanktion som inte är böter eller annan rättsverkan av brott,
2. stipuleras i författning och alltså utgöra ett generellt hot, och
3. tillfalla det allmänna.⁹

⁹ Wiveka Warnling-Nerep, Sanktionsavgifter – särskilt i näringsverksamhet, s. 15.

Det rör sig alltså om en straffliknande ekonomisk sanktion med ett avskräckande och bestraffande syfte. Sanktionsavgifter intar en mellanställning mellan egentliga avgifter och brottspåföljder, vilket kan få betydelse för tillämpningen av såväl regeringsformen som Europakonventionen. Den nu rådande inställningen i doktrinen är att påförande av sanktionsavgifter normalt ska presumeras utgöra brottsanklagelser i konventionens mening och jämföras med böter i normgivningshänseende. Detta medför att de rättssäkerhetsgarantier som uppställs i artikel 6 i Europakonventionen måste vara uppfyllda och att bestämmelser om sanktionsavgifter omfattas av lagkrav med möjlighet till delegation enligt 8 kap. 3 § regeringsformen.¹⁰

18.5.2 Viten och sanktionsavgifter mot det allmänna

Enligt direktiven ska vi i denna del göra en jämförelse med vad som gäller för det allmännas skyldigheter att betala viten i allmänhet, miljö-sanktionsavgifter och sanktionsavgifter på arbetsmiljöområdet. Vi har valt att även redogöra för regleringen kring en annan sanktionsavgift, nämligen upphandlingskadeavgiften.

Vite

Ett vite har alltid anknytning till ett visst föreläggande eller förbud och riktas mot den i beslutet namngivna adressaten. Syftet med ett vite är att verka preventivt och på förhand få en fysisk eller juridisk person att följa ett visst föreläggande eller förbud, inte att som sanktionsavgifterna verka repressivt som en påföljd mot överträdelser mot generella normer.¹¹ Föreläggande och utdömande av vite regleras i lagen (1985:206) om viten, fortsättningsvis benämnd viteslagen.

Viteslagen ställer inte upp några begränsningar när det gäller utdömande av vite mot det allmänna. I lagens andra paragraf anges bara att ett vitesföreläggande ska vara riktat till en eller flera namngivna fysiska eller juridiska personer. Det anses dock vara en vedertagen princip att staten inte föreläggs vite utan särskild reglering.¹² Huvudargu-

¹⁰ Warling-Nerep s.119 och 153 f. samt SOU 2013:38 s. 455.

¹¹ Lavin, Viteslagstiftningen (12 november 2015, Zeteo), kommentaren till 1 § lagen om viten.

¹² Prop. 2012/13:143 s. 66 f.

menten mot att staten ska kunna åläggas vite har varit dels att en statlig myndighet ändå kan beräknas följa ett föreläggande, dels att ett effektivt vite mot staten är nästan omöjligt att åstadkomma eftersom ett utdömt vite i slutänden ändå tillfaller staten.¹³ I vissa författningar framgår det uttryckligen att vite inte kan föreläggas staten, se t.ex. 9 kap. 8 § andra stycket rättegångsbalken och 2 kap. 27 § utsökningsbalken.

Om det finns särskilt författningsstöd kan vite dock riktas mot staten. I 4 kap. 5 § diskrimineringslagen (2008:567) och 7 kap. 7 § arbetsmiljölagen (1977:1160) finns uttryckliga föreskrifter om att ett vitesföreläggande kan riktas även mot staten som arbetsgivare eller som huvudman för utbildningsverksamhet. I förarbetena till diskrimineringslagen hänvisades till motsvarande fråga i förarbetena till den numera upphävda jämställdhetslagen (1991:433), där regeringen ansåg att frågorna om jämställdhet och mångfald i arbetslivet är av sådan vikt att den restriktiva inställningen till vite mot staten borde frångås. Regeringen menade att en ordning där statliga arbetsgivare hålls utanför området där viten kan föreläggas skulle innebära att mer förmånliga regler gällde för dessa än för kommunala eller privata arbetsgivare. En sådan skillnad ansågs inte motiverad. Intresset av ett väl fungerande aktivt arbete för jämställdhet och mångfald även i förhållande till statliga arbetsgivare ansågs vara så starkt att det fanns skäl att markera att även staten skulle kunna föreläggas vite.¹⁴ Liknande argument framfördes i förarbetena till nämnda bestämmelse i arbetsmiljölagen.¹⁵

Ett annat exempel på när vitesföreläggande kan ådömas myndigheter är möjligheten för JO att enligt 21 § andra stycket lagen (1986:765) med instruktion för Riksdagens ombudsmän förelägga vite om högst 10 000 kronor när ombudsmännen inom ramen för sin tillsyn begär upplysningar och yttranden som domstolar, förvaltningsmyndigheter samt anställda hos staten eller kommun eller annan som står under en ombudsmans tillsyn är skyldiga att lämna enligt 13 kap. 6 § andra stycket regeringsformen. Utöver dessa exempel finns sådana där staten kan och ska åläggas vite i fall då staten uppträder som privat subjekt, t.ex. i egenskap av fastighetsägare, nytt-

¹³ Strömberg – Lundell, Allmän förvaltningsrätt, 26 upplagan s. 148.

¹⁴ Prop. 2007/08:95 s. 349 f.

¹⁵ Prop. 2012/13:143 s. 67.

janderättshavare eller ansvarig för rörelse.¹⁶ Det finns också bestämmelser som uttryckligen anger att en kommun kan vara adressat för ett vitesföreläggande, t.ex. 51 § lagen 2006:412 om allmänna vattentjänster.

Informationshanteringsutredningen bedömde i sitt betänkande att tillsynsmyndigheten inte skulle ha befogenhet att rikta vitesförelägganden mot vare sig statliga eller kommunala myndigheter enligt den föreslagna myndighetsdatalagen. Utredningen uttalade i det sammanhanget bland annat att eftersom statliga myndigheters behandling av personuppgifter sker i en verksamhet som i allmänhet inte förekommer utanför det allmänna och som omgärdas av helt andra krav och regler än vad som annars är fallet, fanns inga bärande skäl för att i alla delar ha samma sanktionsmöjligheter mot både myndigheter och enskilda. Utredningen ansåg därför inte att myndigheters behandling av personuppgifter utgjorde ett sådant undantagsfall att man borde avvika från den allmänna rättsgrundsatsen att staten inte kan rikta viten mot sig själv.¹⁷

Enligt 3 § viteslagen ska ett vite fastställas till ett belopp som med hänsyn till vad som är känt om adressatens ekonomiska förhållanden och till omständigheterna i övrigt kan antas förmå honom att följa det föreläggande som är förenat med vitet. Beloppet ska vara tillräckligt stort för att bryta den enskildes motstånd, att jämföra med storleken av ett bötesbelopp som snarare blir beroende av bland annat omfattningen av den enskildes skuld.¹⁸ Vitesbeloppen kan variera kraftigt beroende på sammanhang. Det finns exempel på att viten har satts till allt från tusen kronor till miljonbelopp.¹⁹

Frågor om utdömande av viten prövas enligt 6 § viteslagen av förvaltningsrätt på ansökan av den myndighet som har utfärdat vitesföreläggandet eller, om detta har skett efter överklagande i frågan om vitesföreläggande, av den myndighet som har prövat denna fråga i första instans. I vissa undantagssituationer kan vitesfrågan enligt 7 § viteslagen prövas av allmän domstol.

¹⁶ Lavin, Viteslagstiftningen, Viteslagstiftningen (12 november 2015, Zeteo), kommentaren till 2 § lagen om viten.

¹⁷ SOU 2015:39 s. 631 f.

¹⁸ Lavin, Viteslagstiftningen (12 november 2015, Zeteo), kommentaren till 3 § lagen om viten.

¹⁹ Se exempelvis Högsta domstolens bedömning angående vitets storlek i NJA 1991 s. 200.

Miljösanktionsavgifter

Miljösanktionsavgifter regleras främst i 30 kap. miljöbalken och förordningen (2012:259) om miljösanktionsavgifter. Syftet med avgifterna är att verka repressivt och avskräckande och därmed bidra till att upprätthålla en hög standard i miljöpåverkande verksamhet.²⁰ Miljösanktionsavgifter kan beslutas mot både näringsidkare, myndigheter och enskilda som bedriver verksamhet som faller inom ramen för miljöbalken. Myndigheternas verksamhet faller alltså inte utanför tillämpningsområdet.

Enligt 30 kap. 1 § miljöbalken får regeringen meddela föreskrifter om att miljösanktionsavgift ska betalas bland annat av den som påbörjar en verksamhet som är tillståndspliktig utan att tillstånd har getts eller av den som åsidosätter villkor eller andra bestämmelser i ett tillstånd. Genom förordningen om miljösanktionsavgifter har regeringen meddelat sådana föreskrifter, exempelvis när det gäller miljöfarlig verksamhet och hälsoskydd.

Det har förtydligats i praxis att miljösanktionsavgifter inte kan beslutas mot en myndighet för åsidosättande som har skett vid myndighetsutövning.²¹ När en verksamhet har inslag av både myndighetsutövning och näringsverksamhet har domstolen gjort en bedömning av vilket inslag som är det dominerande för att avgöra om en miljösanktionsavgift kan beslutas.²²

Enligt 30 kap. 1 § miljöbalken ska avgiftens storlek framgå av regeringens föreskrifter, och uppgå till minst 1 000 kronor och högst 1 000 000 kronor. När avgiftens storlek bestäms, ska hänsyn tas till överträdelsens allvar och betydelsen av den bestämmelse som överträdelsen avser. De avgifter som bestäms i förordningen om miljösanktionsavgifter varierar mellan 1 000 och 50 000 kronor. Det är tillsynsmyndigheten som enligt 30 kap. 3 § miljöbalken beslutar om miljösanktionsavgift. Beslutet kan enligt 30 kap. 7 § överklagas till mark- och miljödomstol.

²⁰ Prop. 1997/98:45 del I s. 535.

²¹ MÖD 2001:23.

²² MÖD 2001:21.

Sanktionsavgifter på arbetsmiljöområdet

Enligt 8 kap. 5 § arbetsmiljölagen finns en möjlighet för regeringen eller den myndighet regeringen bestämmer att föreskriva om sanktionsavgifter för vissa typer av överträdelser mot lagen. Avgiften ska vara lägst 1 000 och högst 1 000 000 kronor. Av 18 § 4 arbetsmiljöförordningen (1977:1166) framgår att Arbetsmiljöverket bemyndigats att meddela sådana föreskrifter. De avgifter som bestäms i föreskrifterna varierar mellan 2 000 kronor och 1 000 000 kronor.

De sanktionsavgifter som har föreskrivits på arbetsmiljöområdet riktar sig mot arbetsgivare utan att statliga eller kommunala myndigheter undantas. Bakgrunden till att sanktionsavgifter infördes som huvudsaklig sanktion i stället för de straffbestämmelser som tidigare gällde, var att överträdelser av arbetsmiljöbestämmelser ofta görs inom ramen för verksamhet där många människor medverkar och att det ansågs svårt att utreda en utpekad gärningsmans personliga skuld. Det anfördes i motiven att det t.ex. kan vara osäkert vilket reellt inflytande över händelseförloppet någon som varit formellt ansvarig haft samt att det ofta är uppenbart att bristen i arbetsmiljön är resultatet av att någon inom företaget har gjort sig skyldig till en vårdslöshet utan att man kan peka på vem som gjort det.²³

Avgiften, som enligt 8 kap. 6 § arbetsmiljölagen tillfaller staten, ska enligt 8 kap. 7 § prövas av Arbetsmiljöverket, som sedan kan ansöka hos den förvaltningsrätt inom vars domkrets avgiftsföreläggandet har utfärdats om att sanktionsavgift ska tas ut, om avgiftsföreläggandet inte har godkänts inom utsatt tid.

Upphandlingsskadeavgifter

Ett exempel på sanktionsavgifter som särskilt riktar sig mot myndigheter är reglerna om upphandlingsskadeavgift i lagen (2016:1145) om offentlig upphandling (LOU). Allmän förvaltningsdomstol får efter ansökan från tillsynsmyndigheten enligt 21 kap. 1 och 2 §§ LOU besluta att en upphandlande myndighet ska betala en upphandlingsskadeavgift. Avgiften kan tas ut oberoende av om överträdelserna har skett uppsåtligt eller av oaktsamhet.

²³ Prop. 1993/94:186 s. 49.

En upphandlingsskadeavgift ska enligt 21 kap. 4 § LOU uppgå till lägst 10 000 kronor och högst 10 000 000 kronor. Avgiften får emellertid inte överstiga tio procent av upphandlingens värde. Enligt 21 kap. 5 § LOU ska vid fastställande av upphandlingsskadeavgiftens storlek särskild hänsyn tas till hur allvarlig överträdelsen är. Upphandlingsavgiften ska enligt 21 kap. 8 § LOU tillfalla staten.

När det gäller frågan om möjligheten att ålägga statliga och kommunala myndigheter skyldighet att erlagga avgiften till staten konstaterades i förarbetena till den numera upphävda lagen (2007:1091) om offentlig upphandling att andra liknande avgifter såsom konkurrensskadeavgift och marknadsstörsavgift kan tas ut av offentlighetsrättsliga subjekt om de är att betrakta som näringsidkare. Vidare betonades vikten av att sanktionsbestämmelserna är desamma för alla slag av upphandlande myndigheter och enheter och att något undantag för statliga myndigheter därför inte borde göras. Lagrådet angav vidare i sitt yttrande över förslaget att för att den eftersträlvade preventiva effekten ska uppnås beträffande statliga myndigheter är det viktigt att det upprätthålls en strikt budgetdisciplin, så att avgiften blir kännbar också för en felande statlig myndighet. När det gäller kommunala myndigheter påpekades bland annat att möjligheter att påföra kommuner sanktionsavgifter som tillfaller staten redan förekommer i andra författningar, såsom exempelvis socialtjänstlagen.²⁴

18.5.3 Överväganden och förslag

Utredningens förslag: Sanktionsavgifter ska få tas ut även av statliga och kommunala myndigheter.

För mindre allvarliga överträdelser ska avgiften uppgå till högst 10 000 000 kronor och för allvarligare överträdelser till högst 20 000 000 kronor. Vid bestämmandet av avgiftens storlek i det enskilda fallet ska dataskyddsförordningens bestämmelser tillämpas.

Utgångspunkten för våra överväganden i denna del är att det följer direkt av förordningen att sanktionsavgifter kommer att kunna

²⁴ Prop. 2009/10:180 s. 200.

påföras aktörer i den privata sektorn. Det finns enligt vår mening starka skäl som talar för att sanktionsmöjligheterna bör vara desamma mot privata subjekt som mot myndigheter när det gäller överträdelser mot dataskyddsförordningen.

Inledningsvis kan det konstateras att regleringen syftar till att skydda enskildas integritet, och att enskildas intresse av skydd för sin personliga integritet väger lika tungt om uppgifter behandlas i det allmännas verksamhet som i den privata sektorn. Såväl statliga som kommunala myndigheter hanterar mycket stora mängder personuppgifter, ofta mycket känsliga sådana, som dessutom i allt ökande grad utbyts över myndighets- och nationsgränser utan enskildas samtycke.

Trots att det allmännas verksamhet i och för sig är reglerad i högre grad genom annan lagstiftning än personuppgiftsrelaterad sådan, exempelvis i tryckfrihetsförordningen, offentlighets- och sekretesslagen och arkivlagstiftningen, sker själva behandlingen av personuppgifter på i stort sett samma villkor och enligt samma regelverk som för personuppgiftsansvariga i privat sektor. Det framgår vidare av tillsynsmyndigheternas granskningar under senare år att några av de grövre överträdelserna mot dataskyddslagstiftningens grundläggande principer har gjorts av myndigheter.²⁵ Det är alltså högst tveksamt om myndigheter i allmänhet kan förväntas att i högre grad än enskilda följa regleringen om dataskydd. Inte heller borde behovet av avskräckande sanktioner vara mindre när det gäller myndigheternas personuppgiftsbehandling.

Argumenten mot att sanktionsavgifter enligt förordningen ska kunna tas ut av myndigheter är främst sanktionens bristande effektivitet när det är statliga myndigheter som gör sig skyldiga till överträdelser, samt att – i motsats till den privata sektorn – tjänstefelansvaret utgör ett visst skydd mot att enskilda tjänstemän i offentlig verksamhet gör sig skyldiga till grövre överträdelser. Som framgår av redogörelsen i föregående avsnitt är det trots detta inte helt ovanligt med viten och sanktionsavgifter som riktar sig till statliga och kommunala myndigheter.

²⁵ Se exempelvis Säkerhets- och integritetsskyddsnämndens uttalande om det s.k. kringresande-registret (dnr 173-2013) och Datainspektionens beslut om det s.k. kvinnoregistret (dnr 2790-2014).

Den EU-rättsliga regleringen av personuppgiftsbehandling utgår från det förhållandet att individens rätt till skydd vid behandling av personuppgifter är en grundläggande rättighet enligt artikel 8.1 i Europeiska unionens stadga om de grundläggande rättigheterna. Frågan om vilka sanktioner som bör kunna riktas mot myndigheter bör därför i likhet med andra områden där regleringen framför allt syftar till skydd för individers grundläggande rättigheter, såsom exempelvis inom diskrimineringslagstiftningen, besvaras utifrån ett individperspektiv. Behovet av skydd kan enligt vår mening inte anses vara mindre vid personuppgiftsbehandling som utförs av myndigheter än av enskilda. Tjänstefelsansvar eller disciplinansvar är inte tillräckligt effektiva sanktioner mot systematiska överträdelser på myndighetsnivå för att motivera en annan bedömning. I detta sammanhang förtjänar det att noteras att kommissionen har föreslagit att sanktionsavgifter ska kunna tas ut av EU-institutionerna och andra gemenskapsorgan vid överträdelser mot den förordning som reglerar institutionernas och gemenskapsorganens egen behandling av personuppgifter, parallellt med disciplinära påföljder.²⁶

Inte heller effektivitetsargument leder till ett annat ställningstagande eftersom liknande avgifter har ansetts utgöra en effektiv sanktion på flera andra områden trots att vitet eller avgiften betalas av statliga myndigheter till staten. Här får, såsom anfördes i förarbetena till regleringen om upphandlingsskadeavgifter, förutsättas att budgetdisciplinen upprätthålls så att avgiften får den avskräckande funktion förordningen förutsätter.

Sammanfattningsvis menar vi att övervägande skäl talar för att administrativa sanktionsavgifter ska kunna tas ut av statliga och kommunala myndigheter. I förordningens artikel 83.1–3 anges vilka omständigheter som ska beaktas vid beslut om att ta ut sanktionsavgifter och vid bestämmande av beloppets storlek. Dessa bestämmelser bör enligt vår mening tillämpas även då sanktionsavgifter tas ut av myndigheter.

Bestämmelsen i artikel 83.7 om medlemsstaternas möjligheter att bestämma *i vilken utsträckning* myndigheter ska kunna påföras avgifter, innebär enligt vår mening att medlemsstaterna har utrymme att bestämma ett tak för de belopp som kan påföras myndig-

²⁶ Artiklarna 66 och 69 i kommissionens förslag av den 10 januari 2017, COM(2017) 8 final, 2017/0002 (COD).

heter, på samma sätt som föreslås i betänkandet Brottsdatalog, SOU 2017:29.

När det gäller frågan om sådana beloppstak bör införas för myndigheternas del bör följande beaktas. Som vi har anfört ovan anser vi att ur ett integritetsperspektiv bör samma typ av överträdelse leda till samma typ av sanktion oavsett om överträdelsen begåtts av en myndighet eller ett privat subjekt. Vi anser dock att sanktionsavgifter som påförs myndigheter beloppsmässigt bör ligga i paritet med andra sanktionsavgifter i svensk rätt. Varken på miljöområdet eller på arbetsmiljöområdet är de avgifter som kan tas ut tillnärmelsevis så höga som de som anges i dataskyddsförordningen. Det högsta belopp som kan beslutas vid en överträdelse inom dessa områden är 1 000 000 kronor. Inte heller företagsbot eller upphandlingsskadeavgift kan uppgå till lika höga belopp som enligt förordningen. För företagsbot är minimibeloppet i dag 5 000 kronor och maximibeloppet 10 000 000 kronor. För upphandlingsskadeavgift enligt lagen om offentlig upphandling är lägsta beloppet 10 000 kronor och det högsta 10 000 000 kronor. Avgiften får dock aldrig överstiga en viss procentsats av upphandlingens värde.

Skillnader mellan sanktionsavgifternas storlek utanför respektive innanför myndighetssfären kan också motiveras av att personuppgiftsansvariga i den privata sektorn kan vara multinationella företag där det krävs synnerligen höga sanktionsbelopp för att avgiften ska vara kännbar. För myndigheter kan även en något lägre avgift förväntas påverka agerandet i önskad riktning. Till det kommer att ett felaktigt agerande från en myndighet sällan föranleds av en önskan att maximera vinst eller att göra en större besparing, även om det inte kan uteslutas att det finns ekonomiska motiv. Lägre men tillräckligt kännbara belopp torde därför påverka myndigheterna så länge budgetdisciplinen upprätthålls och de inte får ekonomiska tillskott för att kunna betala sina sanktionsavgifter. Här kan också noteras att i kommissionens förslag till den förordning som reglerar institutionernas och gemenskapsorganens egen behandling av personuppgifter sätts beloppsgränsen för sanktionsavgifterna betydligt lägre än enligt dataskyddsförordningen.²⁷

²⁷ Artikel 66.2 och 66.3 i kommissionens förslag av den 10 januari 2017, COM(2017) 8 final, 2017/0002 (COD).

Ett av huvudsyftena med sanktionsavgifter är att de ska vara effektiva och avskräckande. För att regleringen ska få en tillräckligt avskräckande effekt krävs, trots det som sagts ovan om myndigheters relativt sett högre känslighet även för låga sanktionsavgifter, enligt vår bedömning att maximibeloppet sätts relativt högt. Sammanfattningsvis anser vi att maxbeloppet för sanktionsavgifter mot myndigheter bör ligga i linje med de sanktionsavgifter som i dag finns på andra områden och med storleken på företagsbot, och därmed bestämmas till ett lägre belopp än enligt dataskyddsförordningen.

Sanktionsavgift ska enligt förordningen tas ut på två olika nivåer – en lägre nivå vid överträdelse som betraktas som mindre allvarliga och en högre nivå vid allvarligare överträdelse och underlåtenhet att följa förelägganden eller beslut av tillsynsmyndigheten eller att på annat sätt bistå den. Vi anser att det även för myndigheter finns skäl att ha två olika avgiftsnivåer. Ett maximibelopp om 10 000 000 kronor för mindre allvarliga överträdelse, vilket motsvarar vad som i dag gäller för företagsbot, får anses tillräckligt betydande för att utgöra en kännbar sanktion.

Det finns, utifrån förordningens modell, skäl att bestämma beloppen för allvarligare överträdelse till det dubbla. Det innebär att maximibeloppet för sådana överträdelse bör vara 20 000 000 kronor. Vid bestämmandet av vad som utgör en mindre allvarlig respektive en allvarlig överträdelse bör förordningens artikel 83.4 respektive 83.5 gälla.

Frågan om det närmare förfarandet vid beslut om sanktionsavgifter och effektiva rättsmedel för de som påförs avgifterna behandlas i avsnitt 19.5.3 och 19.7.3.

18.6 Övriga sanktioner och förbudet mot dubbelbestraffning

18.6.1 Medlemsstaternas åligganden

Som nämnts ovan anges i artikel 84 att medlemsstaterna *ska* fastställa regler om andra sanktioner för överträdelse av förordningen, särskilt för överträdelse som inte är föremål för administrativa sanktionsavgifter. Medlemsstaterna har enligt samma artikel att se till att sanktionerna är effektiva, proportionella och avskräckande. Frågan är då vad detta innebär för våra skyldigheter när det gäller genom-

förande. I skäl 152 anges att om förordningen inte harmoniserar administrativa sanktioner eller om nödvändigt i andra fall bör medlemsstaterna genomföra ett system med effektiva, proportionella och avskräckande sanktioner, som kan vara av administrativ eller straffrättslig art. Artikel 84 får alltså tolkas så att om sanktioner saknas enligt förordningen åligger det i princip medlemsstaterna att tappa till sådana luckor, men att det finns relativt stor frihet för medlemsstaterna att avgöra på vilket sätt detta ska ske.

Som framgår av genomgången ovan av förordningens reglering om sanktionsavgifter täcker den det stora flertalet rättigheter och skyldigheter enligt förordningen, med det viktiga undantaget att överträdelse mot artikel 10 inte omfattas.

18.6.2 Allmänt om kriminalisering

Det finns en uttalad politisk vilja att använda straffrätten återhållsamt. Detta eftersom kriminalisering innebär påtagliga inskränkningar i medborgarnas valfrihet och ingripande tvångsåtgärder mot dem som begår brott. Straffrättsliga sanktioner ses vidare som ineffektiva i många fall, i synnerhet när det i första hand är juridiska personer som kan antas göra sig skyldiga till överträdelse av olika slag genom beslut som fattas på viss nivå i organisationen.²⁸

Åklagarutredningen manade i sitt betänkande, SOU 1992:61, till försiktighet vid användandet av kriminalisering som metod för att styra medborgarnas beteende. Utredningen fastslog vissa kriterier för att en kriminalisering ska framstå som befogad, bland annat att alternativa sanktioner inte står till buds, inte skulle vara rationella eller skulle kräva oproportionerligt höga kostnader och att straffsanktionen utgör ett effektivt medel för att motverka det icke önskvärda beteendet. Den restriktiva syn på kriminalisering som kom till uttryck i utredningen och den efterföljande propositionen fick i huvudsak stöd vid riksdagsbehandlingen.²⁹

Straffrättsanvändningsutredningen fick i uppdrag av regeringen att på nytt analysera och ta ställning till vilka kriterier som bör gälla för att kriminalisering ska anses vara befogad, se dir. 2011:31. Som

²⁸ SOU 2013:38 s. 536.

²⁹ Prop. 1994/95:23 s. 52 f., bet. 1994/95:juU2 och rskr. 1994/95:40.

utgångspunkt angavs att kriminalisering bör ske med återhållsamhet och endast användas när den metoden som framstår som den mest effektiva för att motverka det oönskade beteendet. Utredningen tog fram fem kriterier som den ansåg ska vara uppfyllda för att kriminalisering ska komma i fråga. Dessa kan sammanfattas enligt följande.

1. Det tänkta straffbudet måste avse ett identifierat och konkretiserat intresse som är skyddsvärt (godtagbart skyddsintresse).
2. Det beteende som avses bli kriminaliserat måste kunna orsaka skada eller fara för skada på skyddsintresset.
3. Endast den som har visat skuld – varit klandervärd – bör träffas av straffansvar, vilket innebär att kriminaliseringen inte får äventyra tillämpningen av skuldprincipen.
4. Det får inte finnas något tillräckligt värdefullt motstående intresse.
5. Det får inte finnas någon alternativ metod som är tillräckligt effektiv för att komma till rätta med det oönskade beteendet. I första hand bör vite, sanktionsavgift eller återkallelse av tillstånd övervägas. Straff bör väljas i sista hand.³⁰

Utredningen ansåg att för att inte riskera att komma i konflikt med det så kallade dubbelbestraffningsförbudet (se vidare nedan) bör sådana beteenden som sanktioneras med avgift inte samtidigt vara straffbelagda. Visserligen kan man med åtalsbegränsningsregler, jämningsregler, inskränkning av anmälningsplikt osv. försöka se till att dubbelbestraffningsförbudet inte överträds i praktiken, men en sådan uppbyggnad av regelverket gör enligt utredningen att detta blir svårt att överblicka och besvärligt att tillämpa. Utredningen ansåg vidare att det bör vara möjligt för den enskilde att kunna förutse om ett visst beteende leder till straff eller avgift, och förordade därför att när sanktionsavgift införs för beteenden som redan är straffbelagda, dessa beteenden avkriminaliseras i motsvarande mån.³¹ Straffrättsanvändningsutredningens betänkande har remissbehandlats och bereds nu inom Regeringskansliet.

³⁰ SOU 2013:38 s. 498.

³¹ SOU 2013:38 s. 546 f.

18.6.3 Dubbelprövningsförbudet

Europakonventionen gäller som lag i Sverige. I konventionen regleras mänskliga rättigheter såsom rätten till en rättvis rättegång i artikel 6. I artikel 4.1 i det sjunde tilläggsprotokollet till konventionen regleras rättigheten att inte bli lagförd eller straffad två gånger, ibland kallat dubbelbestraffningsförbudet. Fortsättningsvis kommer här att användas den något mer korrekta termen dubbelprövningsförbudet.

Det svenska systemet med samtidig tillämpning av en administrativ sanktion i form av skattetillägg och en straffrättslig sanktion i form av skattebrott har prövats i domen *Lucky Dev* mot Sverige (no. 7356/10, den 27 november 2014), där Europadomstolen fann att en kränkning av dubbelprövningsförbudet hade skett.

Dubbelprövningsförbudet finns även reglerat i EU-rätten, närmare bestämt i artikel 50 i Europeiska unionens stadga om de grundläggande rättigheterna. EU-domstolen har i ett avgörande år 2013 ansett sig behörig att pröva de svenska skattetilläggs- och skattebrottsreglerna såvitt de gäller mervärdesskatt, men lämnade i domen över till den frågande tingsrätten att bedöma om förfarandet stred mot dubbelprövningsförbudet.³² Högsta domstolen och Högsta förvaltningsdomstolen har under 2013 ändrat sin tidigare praxis och nu kommit fram till att det svenska systemet med två förfaranden och dubbla sanktioner vid oriktiga uppgifter i skatteförfarandet är oförenligt med dubbelprövningsförbudet.³³

18.6.4 Överväganden och förslag

Utredningens förslag: Sanktionsavgifter enligt artikel 83 i dataskyddsförordningen ska kunna tas ut även vid överträdelser av artikel 10 i förordningen. Avgiftens storlek ska bestämmas inom ramen för den högre beloppsgräns som gäller för överträdelser mot bland annat bestämmelserna om känsliga personuppgifter.

³² Dom Åkerberg Fransson, C-617/10, EU:C:2013:280.

³³ NJA 2013 s. 502, NJA 2013 s. 746 och HFD 2013 ref. 71. Jfr Europadomstolens dom i A och B mot Norge, (no 24130/11 och 29758/11, den 15 november 2016).

Utredningens bedömning: Något straff ska inte ådömas den som bryter mot förordningen.

Någon möjlighet för tillsynsmyndigheten att förena sina förelägganden med vite bör inte införas.

Sanktionsavgift vid överträdelser mot artikel 10

Dataskyddsförordningens artikel 10 begränsar möjligheterna att behandla uppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder, och innebär alltså skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden att se till att behandling bara sker i tillåtna fall. Intresset av att upprätthålla efterlevnaden av de begränsningar som anges i artikel 10, dvs. möjligheterna att behandla personuppgifter om fällande domar och överträdelser som rör brott, väger enligt vår mening lika tungt ur integritetssynpunkt som att säkerställa efterlevnaden av förbudet mot behandling av vissa typer av känsliga personuppgifter. Behandling av uppgifter om misstänkta eller lagförda brott uppfattas många gånger som mycket integritetskänsligt och stigmatiserande av den registrerade. Som nämnts ovan framstår det inte heller som osannolikt att avsikten varit att även artikel 10 skulle omfattats av regleringen om sanktionsavgifter.

Av förordningens skäl 152 och artikel 84 kan utläsas att det står medlemsstaterna fritt att införa administrativa sanktioner på områden som inte harmoniseras i förordningen. Vår bedömning är att samma system för sanktionsavgifter bör gälla vid överträdelser av artikel 10 som för överträdelser av regleringen om känsliga personuppgifter i artikel 9. Tillsynsmyndigheten bör därför kunna påföra administrativa sanktionsavgifter upp till det högre maxbeloppet även vid överträdelser mot förordningens artikel 10.

Straff

Den befintliga bestämmelsen i 49 § PUL har som nämnts ovan tillämpats sparsamt under senare tid. I många fall är det svårt att peka ut en fysisk person som uppfyller de objektiva och subjektiva rekvisiten för brott och därför är det svårt att fälla någon till ansvar.

Eftersom ansvaret för överträdelser enligt förordningen i huvudsak läggs på personuppgiftsansvariga och personuppgiftsbiträden, vilka i flertalet fall är juridiska personer, bör de mycket kännbara avgifter som kan påföras enligt förordningen vara väsentligt mer effektiva i den meningen att de har en mer avhållande effekt än straffrättsliga sanktioner.

Överträdelser mot förordningen kommer sannolikt i stor utsträckning att upptäckas och utredas av tillsynsmyndigheten. Även ur resurssynpunkt är det därför mer effektivt att låta tillsynsmyndigheten sanktionera överträdelserna. Med det kraftfulla och relativt heltäckande system med sanktionsavgifter som införs genom förordningen finns det därför enligt vår bedömning en alternativ metod som är tillräckligt effektiv och avskräckande för att komma till rätta med överträdelser mot förordningen.

Införandet av straff kan också aktualisera dubbelprövningsförbudet och göra det svårt för personuppgiftsansvariga att förutse vilken sanktion som kan komma ifråga för vilken överträdelse. Med den restriktiva syn på kriminalisering som förutsätts i dag, bedömer vi att någon straffsanktion inte bör införas för överträdelser mot förordningen.

Det bör i detta sammanhang återigen erinras om att visst integritetskränkande beteende som innefattar personuppgiftsbehandling kan vara straffsanktionerat enligt andra bestämmelser, såsom exempelvis dataintrång och förtal. Tjänstefelsansvaret kan också komma ifråga vid gärningar som begås av offentliganställda och som innebär överträdelser av dataskyddsregleringen. För närvarande bereds också förslaget om införande av brottet olaga integritetsintrång i Regeringskansliet (SOU 2016:7). En avkriminalisering av brott mot regleringen om dataskydd innebär alltså inte att integritetskränkningar som begås vid personuppgiftsbehandling kommer att sakna straffrättsliga sanktioner.

Andra sanktioner

Dataskyddsförordningen innehåller inte någon indikation på vilka andra sanktioner som avses i artikel 84. Straffanvändningsutredningen har bedömt att de repressiva metoder som står till buds för staten, vid sidan av straff och sanktionsavgifter, främst är vite och

återkallelse av tillstånd.³⁴ Förordningen föreskriver inte något sådant tillståndsförfarande som gör att återkallelse kan användas som sanktion. Frågan om det finns skäl att behålla möjligheten för tillsynsmyndigheten att vitesförelägga i vissa situationer måste dock övervägas i detta sammanhang.

Inledningsvis kan konstateras att Datainspektionen hittills aldrig använt sig av den möjlighet att vitesförelägga som finns enligt personuppgiftslagen. Som nämnts ovan kan sanktionsavgifterna enligt förordningen användas framåtsyftande, dvs. för att säkerställa ett agerande i enlighet med tillsynsmyndighetens pålagor, genom att det erinras om att sanktionsavgifter kan utgå enligt artikel 83.5 e och artikel 83.6 om föreläggandet eller beslutet inte följs. Vi bedömer att denna möjlighet bör fylla tillsynsmyndighetens behov av handlingsdirigerande sanktion, och att det därför inte finns något behov för tillsynsmyndigheten att också kunna förena sina förelägganden med vite på förordningens tillämpningsområde. Det faktum att även vite kan aktualisera dubbelprövningsförbudet om det utdöms för gärningar som också aktualiserar påförande av sanktionsavgifter, talar ytterligare emot att införa en sådan möjlighet.

Vid sidan av systemet med sanktionsavgifter finns också det i det närmaste strikta skadeståndsansvar som gäller enligt förordningens artikel 82. De höga belopp som kan komma att dömas ut vid mer omfattande behandling får också antas ha en avskräckande effekt.

Sammanfattningsvis menar vi att förordningens system med skadestånd och sanktionsavgifter, tillsammans med den reglering som föreslagits ovan avseende artikel 10, uppfyller kraven på effektiva och avskräckande sanktioner för överträdelser av förordningen och att det därför inte finns behov av att införa några andra sanktioner i svensk rätt.

³⁴ SOU 2013:38 s. 537.

18.7 Betalning och verkställighet

18.7.1 Överväganden och förslag

Utredningens förslag: Sanktionsavgifterna ska tillfalla staten och betalas inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft. Om en sanktionsavgift inte betalas ska den lämnas för indrivning.

Som nämnts ovan framgår det inte uttryckligen av dataskyddsförordningen om de sanktionsavgifter som kan komma att tas ut ska betalas till EU eller till medlemsstaterna. Inte heller regleras det i förordningen hur betalningen eller den närmare verkställigheten av avgifterna ska ske.

I avsaknad av reglering i förordningen om vem sanktionsavgifterna tillfaller, måste utgångspunkten vara att avgifterna ska tillfalla staten. Detta bör framgå av dataskyddslagen. Det bör däremot lämnas till regeringen att bestämma till vilken myndighet betalning ska ske.

Föreskrifter om verkställighet av sanktionsavgifter kan meddelas av regeringen eller den myndighet regeringen bestämmer med stöd av 8 kap. 7 § regeringsformen. Någon upplysningsbestämmelse om detta behöver enligt vår bedömning inte tas in i dataskyddslagen. Med stöd av nämnda bestämmelse i regeringsformen bör regeringen meddela föreskrifter om till vilken myndighet betalning ska ske, liksom sedvanliga föreskrifter om betalningen i övrigt, om indrivning och om preskription, i likhet med vad som föreslagits i betänkandet Brottsdatalag, SOU 2017:29.

19 Processuella frågor

19.1 Vårt uppdrag

Enligt kommittédirektiven ska vi analysera i vilken utsträckning det behövs kompletterande bestämmelser om de rättsmedel för enskilda som regleras i dataskyddsförordningen. Vi ska vidare analysera om det behövs kompletterande bestämmelser om sådana integritetsskyddsorganisationer som regleras i förordningen eller om vilandeförklaring eller skadestånd, samt lämna sådana författningsförslag som är behövliga och lämpliga.

Enligt direktiven ska vi även analysera i vilken utsträckning det behövs kompletterande bestämmelser om utövandet av tillsynsmyndighetens befogenheter. Det kan dock konstateras att själva utövandet av befogenheterna har behandlats av Utredningen om tillsynen över den personliga integriteten i betänkandet SOU 2016:65. Den fråga som ankommer på oss att utreda rörande utövandet av tillsynsmyndighetens befogenheter är därmed främst att analysera i vilken utsträckning det behövs kompletterande processuella bestämmelser till skydd för bland andra den personuppgiftsansvarige och de registrerade, i samband med att tillsynsmyndigheten utövar sina befogenheter.

Dataskyddsförordningen innehåller utförliga bestämmelser som förpliktar de nationella tillsynsmyndigheterna att samarbeta med och assistera andra medlemsstaters tillsynsmyndigheter. Detta innefattar bland annat skyldigheter att samråda och utbyta information. Tillsynsmyndigheterna ges också möjlighet och skyldighet att genomföra gemensamma insatser och utredningar, där personal från olika medlemsstaters tillsynsmyndigheter deltar.

Vid gemensamma insatser får en tillsynsmyndighet, i enlighet med nationell rätt, medge företrädare för deltagande tillsynsmyndigheter i andra medlemsstater att utöva tillsynsbefogenheter. I kommittédirek-

tiven anges därför att vi ska bedöma om det bör införas bestämmelser som möjliggör en överföring av den svenska tillsynsmyndighetens befogenheter till en annan medlemsstats tillsynsmyndighet. Vi ska även lämna lämpliga författningsförslag.

19.2 Kapitlets disposition

De processuella frågor som aktualiseras när en behandling av personuppgifter ifrågasätts behandlas i detta kapitel i den kronologiska ordning de normalt uppkommer. Först behandlas således vilka rättsmedel som står till buds för den registrerade i direkt förhållande till den personuppgiftsansvarige eller biträdet, dvs. utan inblandning av tillsynsmyndigheten (avsnitt 19.3). Därefter behandlas den registrerades möjlighet att lämna in klagomål till tillsynsmyndigheten och få ett besked om myndigheten avser att vidta några åtgärder eller inte (avsnitt 19.4). I de påföljande avsnitten behandlas dels frågor som rör tillsynsmyndighetens handläggning av ärenden (avsnitt 19.5) och gemensamma insatser med utländska tillsynsmyndigheter (avsnitt 19.6), dels rätten att överklaga tillsynsmyndighetens beslut (avsnitt 19.7) och andra beslut enligt dataskyddslagen (avsnitt 19.8). Den registrerades möjligheter att få stöd av en ideell organisation behandlas därefter (avsnitt 19.9) och till sist vissa frågor som rör domstolsförfarandet (avsnitt 19.10).

19.3 Rättsmedel mot den personuppgiftsansvarige eller personuppgiftsbiträdet

19.3.1 Gällande rätt

Enligt 28 § PUL är den personuppgiftsansvarige skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med personuppgiftslagen eller föreskrifter som har utfärdats med stöd av lagen.

I 48 § PUL anges att den personuppgiftsansvarige ska ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med personuppgiftslagen har orsakat. Med stöd av denna bestämmelse kan den registrerade ansöka om stämning mot den personuppgiftsansvarige och yrka

att den personuppgiftsansvarige ska åläggas att betala ersättning. Om den personuppgiftsansvarige är en statlig myndighet får begäran om ersättning ges in till Justitiekanslern. Enligt förordningen om handläggning av skadeståndsanspråk mot staten ska Justitiekanslern handlägga sådana anspråk som görs med stöd av personuppgiftslagens skadeståndsbestämmelse.

Om den personuppgiftsansvarige är en myndighet har den registrerade också i vissa fall möjlighet att initiera en process i förvaltningsdomstol. Enligt 52 § PUL får nämligen några av de beslut som myndigheten fattar enligt personuppgiftslagen överklagas till allmän förvaltningsdomstol. Denna rätt gäller endast myndighetens beslut om information enligt 26 § PUL, om rättelse och underrättelse till tredje man enligt 28 §, om information enligt 29 § andra stycket och om upplysningar enligt 42 §. Rätten att överklaga gäller inte beslut som fattats av riksdagen, regeringen eller riksdagens ombudsmän.

19.3.2 Dataskyddsförordningen

Varje registrerad som anser att hans eller hennes rättigheter har åsidosatts som en följd av att hans eller hennes personuppgifter har behandlats på ett sätt som inte är förenligt med förordningen ska ha rätt till ett effektivt rättsmedel, utöver rätten att lämna in ett klagomål till en tillsynsmyndighet (artikel 79.1). Talan mot en personuppgiftsansvarig eller ett personuppgiftsbiträde ska väckas vid domstolarna i den medlemsstat där den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad. Talan får även väckas vid domstolarna i den medlemsstat där den registrerade har sin hemvist, såvida inte den personuppgiftsansvarige eller personuppgiftsbiträdet är en myndighet som agerar inom ramen för sin myndighetsutövning (artikel 79.2).

Artikel 82 innehåller bestämmelser om skadestånd. Enligt artikel 82.6 ska domstolsförfaranden för utövande av rätten till ersättning tas upp vid de domstolar som är behöriga enligt artikel 79.2.

19.3.3 Överväganden och förslag

Utredningens förslag: Om den personuppgiftsansvarige är en myndighet, ska myndighetens beslut avseende behandlingen av personuppgifter i vissa fall få överklagas av den registrerade till allmän förvaltningsdomstol.

Det ska förtydligas i dataskyddslagen att rätten till ersättning enligt dataskyddsförordningen även gäller vid överträdelser av bestämmelser som kompletterar dataskyddsförordningen.

Utredningens bedömning: Den registrerades rätt till ett effektivt rättsmedel mot den personuppgiftsansvarige eller biträdet tillgodoses genom möjligheten att föra talan om skadestånd i allmän domstol.

En registrerad ska enligt dataskyddsförordningen ha rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde. Av kontexten framgår att rättsmedlet ska innefatta en rätt att föra talan i domstol. Vilken slags talan som den registrerade ska kunna väcka framgår däremot inte, vare sig av artikeltexten eller av skälen till förordningen.

Även enligt dataskyddsdirektivet ska den registrerade ha rätt till ett rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde. I artikel 22 i direktivet anges att medlemsstaterna ska föreskriva att var och en har rätt att föra talan inför domstol om sådana kränkningar av rättigheter som skyddas av den nationella lagstiftning som är tillämplig på behandlingen. Vid genomförandet av dataskyddsdirektivet bedömdes att denna bestämmelse var genomförd i svensk rätt genom möjligheten för enskilda att vid allmän domstol föra talan om skadestånd för kränkningar av alla rättigheter som direktivet och den svenska lagstiftningen ger enskilda.¹

¹ Prop. 1997/98:44 s. 106.

En myndighets beslut om personuppgiftsbehandling ska i vissa fall få överklagas till allmän förvaltningsdomstol

Om den personuppgiftsansvarige är en myndighet får enligt gällande rätt vissa av de beslut som myndigheten fattar i denna egenskap överklagas till allmän förvaltningsdomstol (52 § PUL). Denna bestämmelse har inte sin grund i dataskyddsdirektivet, utan motiveras av allmänna förvaltningsrättsliga principer om att förvaltningsbeslut som direkt berör en enskild person ska kunna överprövas av domstol.²

Dessa allmänna förvaltningsrättsliga principer gör sig gällande även avseende vissa av de beslut som personuppgiftsansvariga myndigheter kommer att fatta enligt dataskyddsförordningen, till följd av en begäran av en registrerad. När den personuppgiftsansvarige är en myndighet kan nämligen vissa beslut rörande behandlingen av personuppgifter sägas vara ett utflöde av myndighetens myndighetsutövning. Dataskyddslagen bör därför, i likhet med personuppgiftslagen, förses med en uttrycklig bestämmelse om att vissa myndighetsbeslut får överklagas till allmän förvaltningsdomstol. Prövnings-tillstånd bör krävas för överklagande till kammarrätten.

Rätten att överklaga bör omfatta beslut som en personuppgiftsansvarig myndighet fattar med anledning av att en registrerad utövar sina rättigheter enligt kapitel III i dataskyddsförordningen. De rättigheter som kan föranleda överklagbara beslut rör information (artikel 12.5), registerutdrag m.m. (artikel 15), rättelse (artikel 16), radering (artikel 17), begränsning (artikel 18), underrättelse till tredje man om rättelse, radering eller begränsning (artikel 19) och invändningar (artikel 21). Det bör noteras att överklaganderätten bara kan gälla beslut som är av den karaktären att de är överklagbara enligt allmänna förvaltningsrättsliga principer, jfr t.ex. RÅ 2010 ref. 72 och RÅ 2007 ref. 7. En myndighets faktiska handlande eller underlåtenhet att handla kan exempelvis inte överklagas. En annan förutsättning för överklagande är att beslutet har någon inte alltför obetydlig verkan för parter eller andra. Normalt saknas också möjlighet att klaga över motiveringen till ett beslut.

² Prop. 2005/06:173 s. 51 f.

Den registrerade får föra talan om skadestånd

Den registrerades rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet vid skada som uppstått till följd av behandling som strider mot dataskyddsförordningen regleras i artikel 82. Med behandling som strider mot dataskyddsförordningen avses enligt skäl 146 även behandling som strider mot nationella bestämmelser som specificerar förordningen. Artikel 82, som är direkt tillämplig, tar över de allmänna skadestandsreglerna i skadeståndslagen, jfr 1 kap. 1 § i den lagen.

Domstolsförfaranden rörande skadestånd ska enligt artikel 82.6 tas upp vid de domstolar som är behöriga enligt artikel 79.2, dvs. vid en domstol i den medlemsstat där den personuppgiftsansvarige eller biträdet är etablerad. Såvida den ansvarige eller biträdet inte är en myndighet får talan i stället väckas vid en domstol i den medlemsstat där den registrerade har sin hemvist. Bestämmelsen tar över rättegångsbalkens allmänna forumregler, jfr 10 kap. 21 § rättegångsbalken.

Ersättningen ska enligt förordningen täcka såväl materiell som immateriell skada, dvs. med svenska termer ekonomisk och ideell skada. Kränkning, som i 48 § PUL nämns särskilt vid sidan av skada, utgör en immateriell eller ideell skada.³ Förarbetsuttalanden rörande personuppgiftslagen och den praxis som har utvecklats vid tillämpningen av 48 § PUL bör därför kunna vara vägledande även vid prövning av rätten till ersättning enligt artikel 82 i dataskyddsförordningen. Se även avsnitt 18.3.1.

I likhet med den bedömning som gjordes vid genomförandet av dataskyddsdirektivet anser vi att den registrerades rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde tillgodoses i svensk rätt genom möjligheten att vid allmän domstol föra talan om ersättning för den skada som en behandling av personuppgifter i strid med förordningen har gett upphov till.

Samma rätt till ersättning gäller enligt skäl 146 även vid skada som uppstått genom behandling av personuppgifter i strid med de nationella bestämmelser som specificerar dataskyddsförordningen. Detta bör förtydligas genom en upplysningsbestämmelse i dataskyddslagen. Denna bestämmelse bör erinra om att rätten till ersättning gäller även

³ För en närmare beskrivning av det skadeståndsrättsliga begreppet kränkning, se SOU 2010:87 s. 104 f.

vid överträdelse av bestämmelser i dataskyddslagen och i andra författningar som kompletterar dataskyddsförordningen. Några nationella bestämmelser i övrigt, utöver dem som redan finns i rättegångsbalken och skadeståndslagen, behövs däremot inte för att uppfylla dataskyddsförordningens krav på rättsmedel enligt artikel 79.

19.4 Klagomål till tillsynsmyndigheten

19.4.1 Gällande rätt

Den registrerades möjlighet att ge in ett klagomål till Datainspektionen är inte reglerad i författning. På inspektionens hemsida anges dock att inspektionen tar del av alla klagomål, bedömer om tillsyn ska inledas och lämnar ett besked till den som framfört klagomålet.

19.4.2 Dataskyddsförordningen

Varje registrerad som anser att behandlingen av personuppgifter som avser henne eller honom strider mot dataskyddsförordningen ska ha rätt att lämna in ett klagomål till en tillsynsmyndighet (artikel 77.1). Tillsynsmyndigheten ska underrätta den enskilde bland annat om hur arbetet med klagomålet fortskrider och vad resultatet blir (artikel 77.2).

Om tillsynsmyndigheten underlåter att behandla ett klagomål eller att informera den registrerade inom tre månader om hur det fortskrider med klagomålet eller vilket beslut som har fattats med anledning av det, ska varje registrerad person ska ha rätt till ett effektivt rättsmedel (artikel 78.2).

19.4.3 Överväganden och förslag

Utredningens förslag: Om tillsynsmyndigheten inte inom tre månader behandlar ett klagomål, ska den registrerade kunna begära besked i frågan om tillsynsmyndigheten avser att utöva tillsyn. Myndigheten ska då inom två veckor antingen lämna ett sådant besked eller i ett särskilt beslut avslå begäran om besked. Om tillsynsmyndigheten avslår begäran om besked får den registrerade begära nytt besked i ärendet först efter tre månader.

Utredningens bedömning: Det behövs inga författningsbestämmelser om den registrerades rätt att lämna in klagomål till tillsynsmyndigheten.

Den registrerade får lämna in klagomål till tillsynsmyndigheten

Det finns i gällande svensk rätt inga uttryckliga bestämmelser om rätten att framföra klagomål till Datainspektionen. Inte heller dataskyddsförordningen ger anledning till nationell reglering av rätten att ge in klagomål. Den registrerades rätt regleras direkt i artikel 77 i förordningen och tillsynsmyndighetens skyldighet att handlägga sådana klagomål föreskrivs i artikel 57.1 f. Vi lämnar därför inget författningsförslag i denna del.

Vid utebliven eller långsam handläggning av ett klagomål ska den registrerade kunna begära besked

Tillsynsmyndigheten ansvarar för att behandla klagomål, vilket innefattar en skyldighet att, där så är lämpligt, undersöka den sakfråga som klagomålet gäller. Tillsynsmyndigheten ska också inom rimlig tid underrätta den enskilde om hur undersökningen fortskrider och om resultatet (artikel 57.1 f och artikel 77.2 i dataskyddsförordningen). Om tillsynsmyndigheten inte inom tre månader uppfyller dessa skyldigheter, ska den registrerade ha rätt till ett effektivt rättsmedel.

En motsvarande rätt för enskilda att föra passivitets- eller dröjsmålstalan mot myndigheter som inte agerar inom föreskriven tidsfrist återfinns i flera unionsrättsakter, bland annat inom det finansiella området och i tullagstiftningen. Det har dock inte varit självklart hur denna rätt bäst ska tillgodoses inom ramen för den svenska förvaltningsprocessuella traditionen, eftersom denna innebär att domstolen överprövar ett skriftligt myndighetsbeslut. På flera områden har EU-rättsliga bestämmelser om dröjsmålstalan genomförts på så sätt att den enskilde har getts en möjlighet att hos förvaltningsdomstol begära förklaring att ärendet onödigt uppehålls. Om myndigheten inte har meddelat ett beslut inom en viss tid från det att domstolen

har lämnat en sådan förklaring, ska ansökan anses ha avslagits.⁴ Detta fingerade avslagsbeslut kan därefter överklagas i samma ordning som om ett formellt beslut verkligen hade fattats.

I prop. 2016/17:180, En modern och rättssäker förvaltning – ny förvaltningslag, som bygger på Förvaltningslagsutredningens betänkande (SOU 2010:29), föreslås en lösning som i stället syftar till att framtvunga ett överklagbart beslut i handläggningsfrågan. Enligt det förslaget ska den enskilde inte i första skedet vända sig till förvaltningsdomstol, utan hos myndigheten begära att ärendet avgörs. Myndigheten ska då inom fyra veckor antingen avgöra ärendet eller i ett särskilt beslut avslå framställningen. Ett sådant avslagsbeslut får sedan överklagas till den domstol eller förvaltningsmyndighet som är behörig att pröva ett överklagande av avgörandet i ärendet (se 12 § i förslaget till förvaltningslag). Med tanke på att regeringens förslag, om det så småningom antas av riksdagen, innebär att ett nytt rättsmedel mot långsam myndighetshandläggning införs i Sverige på generell nivå, anser vi att dataskyddsförordningens bestämmelse om dröjsmålstanan bör genomföras på ett sätt som följer samma principiella konstruktion.

Om tillsynsmyndigheten inte behandlar ett klagomål inom den tidsfrist som anges i förordningen, bör myndigheten således vara skyldig att på skriftlig begäran av den registrerade lämna besked i frågan om tillsynsmyndigheten tänker utöva tillsyn eller inte med anledning av klagomålet. Om tillsynsmyndigheten inte kan lämna ett sådant besked inom två veckor, t.ex. på grund av att ärendet kräver ytterligare utredning, bör tillsynsmyndigheten vara skyldig att i ett särskilt beslut avslå den registrerades begäran om besked. Ett sådant avslagsbeslut utgör myndighetsutövning och ska därför enligt 20 § förvaltningslagen innehålla skälen för beslutet. Endast på så sätt skapas förutsättningar för att i domstol göra en prövning av om handläggningstiden hos tillsynsmyndigheten är rimlig, se avsnitt 19.7 om överklagande av tillsynsmyndighetens beslut.

Om tillsynsmyndigheten avslår begäran om besked bör den registrerade ha möjlighet att på nytt begära besked i ärendet. Tillsynsmyndigheten bör dock dessförinnan få en rimlig tid på sig att faktiskt handlägga klagomålet. Enligt vår mening är tre månader en rimlig tids-

⁴ Se t.ex. 6 kap. 26 § tullagen (2016:253) och 26 kap. 2 § lagen (2007:528) om värdepappersmarknaden.

frist. Om en ny begäran om besked kommer in till tillsynsmyndigheten innan tre månader har förflutit sedan myndigheten avslog den första begäran om besked, bör således tillsynsmyndigheten avvisa begäran.

19.5 En rättssäker handläggning hos tillsynsmyndigheten

19.5.1 Gällande rätt

Tillsynsmyndighetens utredningsbefogenheter regleras i 43 § PUL. Enligt denna bestämmelse har tillsynsmyndigheten rätt att för sin tillsyn på begäran få

- a) tillgång till de personuppgifter som behandlas,
- b) upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna, och
- c) tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter.

Tillsynsmyndigheten har inte några maktbefogenheter att ta till om den personuppgiftsansvarige vägrar att t.ex. tillhandahålla information eller bereda myndigheten tillträde till lokalerna. Myndigheten kan inte heller begära handräckning av polisen eller Kronofogdemyndigheten i en sådan situation.

Enligt 44 § PUL får tillsynsmyndigheten vid vite förbjuda den personuppgiftsansvarige att behandla personuppgifter på något annat sätt än genom att lagra dem, om myndigheten efter begäran enligt 43 § inte kan få tillräckligt underlag för att konstatera att behandlingen av personuppgifter är laglig. Detta ansågs vid införandet av personuppgiftslagen som en lämpligare åtgärd än regler om att myndigheten skulle få genomdriva sina rättigheter med t.ex. polishjälp.⁵

Om tillsynsmyndigheten kan konstatera att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt, ska myndigheten enligt 45 § PUL genom påpekanden eller liknande förfaranden

⁵ Prop. 1997/98:44 s. 102 f. och SOU 1997:39 s. 446 f.

försöka åstadkomma rättelse. Går det inte att få rättelse på något annat sätt eller är saken brådskande, får myndigheten vid vite förbjuda den personuppgiftsansvarige att fortsätta att behandla personuppgifterna på något annat sätt än genom att lagra dem. Vite får även föreskrivas om den personuppgiftsansvarige inte frivilligt följer ett beslut om säkerhetsåtgärder enligt 32 § som vunnit laga kraft.

I 46 § första stycket PUL anges att den personuppgiftsansvarige ska ha fått tillfälle att yttra sig innan tillsynsmyndigheten beslutar om vite enligt 44 eller 45 §. Om saken är brådskande, får dock myndigheten i avvaktan på yttrandet meddela ett tillfälligt beslut om vite. Det tillfälliga beslutet ska omprövas, när tiden för yttrande har gått ut.

Tillsynsmyndigheten får inte själv besluta om utplåning av personuppgifter. Enligt 47 § PUL får dock myndigheten ansöka hos förvaltningsrätten om att sådana personuppgifter som har behandlats på ett olagligt sätt ska utplånas. Beslut om utplånande får inte meddelas om det är oskäligt.

19.5.2 Dataskyddsförordningen

Dataskyddsförordningen innehåller direkt tillämpliga bestämmelser om tillsynsmyndighetens befogenheter. Dessa befogenheter är fler, eller i vart fall mer detaljerat reglerade, än dem som anges i personuppgiftslagen. Tillsynsmyndighetens utredningsbefogenheter, som regleras i artikel 58.1 i förordningen, motsvarar i stora drag de befogenheter som tillkommer myndigheten enligt personuppgiftslagen. De s.k. korrigerande befogenheterna, som framgår av artikel 58.2, är däremot mer omfattande. Som exempel kan nämnas att tillsynsmyndigheten enligt led g i den angivna artikeln får förelägga om radering av personuppgifter och att den enligt led i får påföra administrativa sanktionsavgifter. Vidare anges i artikel 58.3 vilken möjlighet myndigheten har att utfärda tillstånd och att ge råd.

Enligt artikel 58.5 ska det i den nationella lagstiftningen fastställas att tillsynsmyndigheten har befogenhet att upplysa de rättsliga myndigheterna om överträdelser av förordningen och vid behov inleda eller på annat vis delta i rättsliga förfaranden, för att verkställa bestämmelserna.

Varje medlemsstat får enligt artikel 58.6 föreskriva att dess tillsynsmyndighet ska ha ytterligare befogenheter, utöver dem som av-

ses i punkterna 1, 2 och 3. Om den svenska myndigheten bör ges sådana ytterligare befogenheter är en fråga som har övervägts av Utredningen om tillsynen över den personliga integriteten. Utredningen har i sitt betänkande konstaterat att det för närvarande inte finns något sådant behov.⁶

I artikel 58.4 anges att utövandet av de befogenheter som tillsynsmyndigheten tilldelas enligt denna artikel ska omfattas av lämpliga skyddsåtgärder, inbegripet effektiva rättsmedel och rättssäkerhet, som fastställs i unionsrätten och i medlemsstaternas nationella rätt i enlighet med stadgan. I artikel 83.8 upprepas kravet på lämpliga skyddsåtgärder avseende tillsynsmyndighetens befogenheter att påföra administrativa sanktionsavgifter. Innebörden av kravet på skyddsåtgärder i tillsynsmyndighetens verksamhet utvecklas i skäl 129 till förordningen.

19.5.3 Överväganden och förslag

Utredningens förslag: Tillsynsmyndighetens befogenheter enligt dataskyddsförordningen ska gälla även vid myndighetens tillsyn över att de bestämmelser som kompletterar förordningen följs.

Innan tillsynsmyndigheten fattar vissa ingripande beslut ska den som beslutet gäller ha fått tillfälle att yttra sig över allt material av betydelse för beslutet, om det inte är uppenbart obehövligt. Om saken är brådskande kan dock ett tillfälligt beslut fattas, i avvaktan på yttrandet.

Sanktionsavgift ska inte få tas ut om den som anspråket riktar mot inte har getts tillfälle att yttra sig inom fem år från det att överträdelsen ägde rum.

Vissa ingripande beslut ska delges, om det inte är uppenbart obehövligt. Vissa former av stämmningsmannadelgivning ska få användas bara om det finns särskild anledning att anta att mottagaren har avvikit eller på annat sätt håller sig undan.

Om det finns skäl att ifrågasätta giltigheten av en unionsrättsakt som påverkar tillämpningen av förordningen, ska tillsynsmyndigheten få ansöka hos förvaltningsrätten om att en tillsynsåtgärd ska vidtas, i stället för att själv besluta om åtgärden.

⁶ SOU 2016:65 s. 154 f.

Utredningens bedömning: Det bör inte införas några bestämmelser om tillsynsmyndighetens tillträde till en personuppgiftsansvarigs eller ett personuppgiftsbiträdes lokaler.

Tillsynsmyndigheten får enligt förordningen förelägga en personuppgiftsansvarig om att uppgifter ska raderas. Det behövs inga bestämmelser om förhandsprövning i domstol.

Förordningens krav på att tillsynsmyndighetens befogenheter ska kringgärdas av skyddsåtgärder innefattar en skyldighet för medlemsstaterna att dels se till att den personuppgiftsansvarige och personuppgiftsbiträdet har tillgång till effektiva rättsmedel, dels skapa förutsättningar för en rättsäker handläggning hos tillsynsmyndigheten. Frågan om effektiva rättsmedel behandlas i avsnitt 19.7. I detta avsnitt behandlas enbart behovet av åtgärder för att säkerställa en rättsäker handläggning hos tillsynsmyndigheten.

Tillsynsmyndighetens ärendehandläggning och verksamhet i övrigt omfattas givetvis av regeringsformens grundsatser om legalitet och objektivitet. Dessutom gäller förvaltningslagens generella bestämmelser om bland annat effektivitet, partsinsyn, kommunicerings- och motiveringsskyldighet – bestämmelser som alla syftar till att stärka rättssäkerheten. Vid utövandet av de flesta av tillsynsmyndighetens befogenheter är dessa allmänna och särskilda krav på god förvaltning tillräckliga för att säkerställa de krav på myndighetsutövningen som ställs i dataskyddsförordningen. Det bör dock övervägas om vissa av de mer ingripande befogenheterna bör föranleda att ytterligare skyddsåtgärder införs. Det bör även övervägas om tillsynsmyndighetens befogenheter att ingripa mot överträdelse av nationella bestämmelser som kompletterar dataskyddsförordningen ska regleras.

Tillsynsmyndighetens befogenheter ska gälla även vid tillsyn enligt dataskyddslagen och sektorsspecifika författningar

Bestämmelsen i artikel 58 om tillsynsmyndighetens befogenheter avser enligt dess lydelse endast tillsynen över tillämpningen av förordningens bestämmelser. För att förordningens intentioner ska få fullt genomslag krävs dock att tillsynsmyndigheten kan vidta samma åtgärder vid sin tillsyn över tillämpningen av de nationella bestämmelser som kompletterar förordningen. Detta bör framgå uttryck-

ligen av dataskyddslagen. Befogenheterna bör gälla oavsett om de kompletterande nationella bestämmelserna har placerats i dataskyddslagen eller om de återfinns i sektorsspecifika författningar som avser behandling av personuppgifter.

Mottagaren måste få tillfälle att yttra sig innan förelägganden beslutas

I 46 § PUL finns bestämmelser som avviker från förvaltningslagen och utgör ytterligare processuella skyddsåtgärder för den personuppgiftsansvarige när tillsynsmyndigheten utövar sin befogenhet att besluta om vitesföreläggande. I paragrafen anges bland annat att den personuppgiftsansvarige, enligt huvudregeln, ska ha fått tillfälle att yttra sig innan tillsynsmyndigheten beslutar om vite. Om saken är brådskande, får myndigheten dock i avvaktan på yttrandet meddela ett tillfälligt beslut om vite. Vidare anges att ett vitesföreläggande ska delges den personuppgiftsansvarige. Vissa former av stämmingsmandelgivning får dock användas bara om det med beaktande av vad som har framkommit i det aktuella delgivningsärendet eller vid andra delgivningsförsök med den personuppgiftsansvarige finns anledning att anta att han eller hon har avvikit eller på annat sätt håller sig undan.

Enligt dataskyddsförordningen ska administrativa sanktionsavgifter tas ut vid underlåtelse att rätta sig efter ett föreläggande som har meddelats av tillsynsmyndigheten (artikel 83.5 e och 85.6). Sanktionsavgiften fyller därmed samma funktion som ett vite. Som framgår av avsnitt 18.6.4 anser vi därför att det inte behöver införas någon möjlighet för tillsynsmyndigheten att förena sina förelägganden med vite. Den omständigheten att underlåtenhet att följa ett föreläggande kan leda till att administrativa sanktionsavgifter tas ut motiverar emellertid enligt vår mening att de processuella skyddsåtgärder som nu kringgärdar tillsynsmyndighetens vitesförelägganden bör gälla för alla förelägganden som myndigheten kan meddela med stöd av artikel 58.2 i dataskyddsförordningen.

Således bör tillsynsmyndigheten, innan ett föreläggande enligt artikel 58.2 i dataskyddsförordningen beslutas, vara skyldig att ge mottagaren möjlighet att yttra sig över allt material av betydelse för föreläggandet, om det inte är uppenbart obehövligt. Om saken är brådskande bör dock myndigheten, i avvaktan på yttrandet, kunna

besluta om tillfällig begränsning av eller förbud mot behandling, i enlighet med artikel 58.2 f i dataskyddsförordningen. Ett sådant beslut ska omprövas, när tiden för yttrande har gått ut.

Förelägganden ska delges

Enligt 46 § andra stycket PUL ska vitesförelägganden delges. Den omständigheten att underlåtenhet att följa ett föreläggande enligt dataskyddsförordningen kan leda till administrativa sanktionsavgifter motiverar ett motsvarande krav på delgivning för alla typer av förelägganden som riktas mot en personuppgiftsansvarig eller ett personuppgiftsbiträde som tillsynsmyndigheten kan besluta enligt artikel 58.2 i förordningen. Tillsynsmyndigheten bör alltså enligt vår mening vara skyldig att se till att ett föreläggande kommer mottagaren till del på något av de sätt som föreskrivs i delgivningslagen (2010:1932). Precis som enligt 46 § PUL bör dock vissa typer av stämmningsmannadelgivning, nämligen sådana som innebär att handlingen överlämnas till en annan person än delgivningsmottagaren, få användas bara om det finns särskild anledning att anta att mottagaren har avvikit eller på annat sätt håller sig undan (jfr 34–37 §§ delgivningslagen).

Förelägganden och andra beslut ska hanteras på samma sätt

Behovet av särskilda processuella skyddsåtgärder, som avviker från förvaltningslagens generella bestämmelser, bör övervägas också avseende andra beslut än förelägganden som tillsynsmyndigheten kan fatta med stöd av artikel 58.2 i dataskyddsförordningen. Inte minst med tanke på att överträdelse av dataskyddsförordningen kan leda till administrativa sanktionsavgifter med höga belopp, är det mycket viktigt att tillsynsmyndigheten kommunicerar materialet i ärendet med den personuppgiftsansvarige eller personuppgiftsbiträdet och ger denne möjlighet att yttra sig innan ett beslut fattas. Detta gäller inte bara vid myndighetsutövning mot enskild utan även om mottagaren är en myndighet. Beslut om tillfällig begränsning av, eller tillfälligt förbud mot, behandling måste dock kunna fattas i avvaktan på yttrande, men ska i så fall omprövas när tiden för yttrande har löpt ut.

I vissa fall kan det vara uppenbart obehövt att låta den som beslutet gäller yttra sig, till exempel om det är mottagaren själv som har lämnat uppgifterna i fråga. Kommunikeringsplikten bör därför inte vara absolut.

Vad gäller delgivning av beslut anges i 21 § förvaltningslagen att en sökande, klagande eller annan part ska underrättas om innehållet i det beslut varigenom myndigheten avgör ärendet, om detta avser myndighetsutövning mot någon enskild. Det är myndigheten som bestämmer om underrättelsen ska ske muntligt, genom vanligt brev, genom delgivning eller på något annat sätt. Underrättelsen ska dock alltid ske skriftligt, om parten begär det. Enligt vår mening bör dock tillsynsmyndighetens beslut enligt artikel 58.2 i förordningen alltid delges i enlighet med delgivningslagens bestämmelser, om det inte är uppenbart obehövt. Vissa former av stämmingsmannadelgivning bör dock inte kunna ske annat än under särskilda omständigheter.

Sammanfattningsvis anser vi således att även andra ingripande beslut än tillsynsmyndighetens förelägganden ska omfattas av processuella skyddsåtgärder som avviker från förvaltningslagens generella bestämmelser. Innan tillsynsmyndigheten meddelar ett föreläggande eller annat beslut enligt artikel 58.2 i dataskyddsförordningen, bör därför den som beslutet riktas mot ha fått tillfälle att yttra sig över allt material av betydelse för beslutet, om det inte är uppenbart obehövt. Om saken är brådskande bör myndigheten, i avvaktan på yttrandet, få besluta att behandlingen av personuppgifter tillfälligt ska begränsas eller förbjudas i enlighet med artikel 58.2 f i dataskyddsförordningen. Ett sådant tillfälligt beslut bör omprövas, när tiden för yttrande har gått ut. Vidare bör ett föreläggande eller annat beslut enligt artikel 58.2 i dataskyddsförordningen delges den som det riktas mot, om det inte är uppenbart obehövt. Delgivning enligt 34–37 §§ delgivningslagen ska få användas bara om det finns särskild anledning att anta att mottagaren har avvikit eller på annat sätt håller sig undan. När det gäller tillsynsbeslut i ärenden som har initierats genom klagomål bör även den som har framställt klagomålet få kännedom om beslutet, lämpligen genom att en kopia av beslutet skickas till denne. Formell delgivning bör dock normalt inte krävas i det fallet.

Administrativa sanktionsavgifter måste tas ut inom fem år

Beslut om administrativa sanktionsavgifter är en särskilt ingripande åtgärd. Sådana beslut bör därför inte få fattas om lång tid har förflutit sedan överträdelsen ägde rum. Någon preskriptionstid anges dock inte i dataskyddsförordningen. En sådan begränsning av tillsynsmyndighetens befogenheter måste i stället anses ingå i medlemsstaternas skyldighet att ställa upp lämpliga skyddsåtgärder för rättssäkerheten i nationell rätt (artikel 58.4). I likhet med vad som gäller för t.ex. miljö-sanktionsavgift och sanktionsavgifter på arbetsmiljöområdet bör det därför föreskrivas att sanktionsavgift inte får tas ut, om den som anspråket riktas mot inte inom fem år från det att överträdelsen ägde rum har getts tillfälle att yttra sig.⁷

Platsundersökning ska inte kunna ske med tvång

Enligt dataskyddsförordningen ska tillsynsmyndigheten från den personuppgiftsansvarige och personuppgiftsbiträdet få tillgång till alla personuppgifter och all information som myndigheten behöver för att kunna fullgöra sina uppgifter (artikel 58.2 e). Tillsynsmyndigheten ska också få tillträde till alla lokaler som tillhör den personuppgiftsansvarige och personuppgiftsbiträdet, inbegripet tillgång till all utrustning och alla andra medel för behandling av personuppgifter (artikel 58.2 f). I skäl 129 till förordningen anges att undersökningsbefogenheten när det gäller tillträde till lokaler bör utövas i enlighet med särskilda krav i medlemsstaternas nationella processrätt, såsom kravet på att inhämta förhandstillstånd från rättsliga myndigheter.

Enligt personuppgiftslagen har tillsynsmyndigheten inte rätt att gå in i den personuppgiftsansvariges eller biträdets lokaler utan dennes medgivande. Tillsynsmyndigheten har inte heller möjlighet att hos någon rättslig instans inhämta tillstånd till en sådan åtgärd. Befogenheten att få tillträde till lokalerna kan därmed sägas vara begränsad av den personuppgiftsansvariges eller biträdets samarbetsvilja, precis som tillgången till information. Vid genomförandet av dataskyddsdirektivet ansågs det olämpligt med regler som innebär att myndigheten skulle få genomdriva sina rättigheter med t.ex. polishjälp, eftersom det skulle kunna leda till ett större intrång i den personliga

⁷ Jfr 30 kap. 6 § miljöbalken och 8 kap. 8 § arbetsmiljölagen.

integriteten än det intrång som myndighetens tillsynsverksamhet syftar till att förebygga.⁸ Risken för att tillsynsmyndigheten skulle förbjuda fortsatt behandling av personuppgifter ansågs medföra att de personuppgiftsansvariga blir tillräckligt benägna att ge myndigheten det underlag den behöver.⁹

Oanmälda tillsynsbesök förekommer i Sverige inom flera olika områden. Det är dock endast i ett fåtal sammanhang som tillsynsmyndigheten har rätt att bereda sig tillträde till lokaler utan innehavarens medgivande. Sådana platsundersökningar får dessutom normalt ske endast efter ansökan hos och medgivande av domstol.¹⁰ Ofta får myndigheten begära handräckning av Kronofogdemyndigheten för att genomföra platsundersökningen.¹¹ Gemensamt för de sammanhang där platsundersökning får genomföras med tvång är att det finns risk för till exempel sabotage eller undanhållande av bevis.

Dataskyddsförordningen ger tillsynsmyndigheten en ovillkorlig rätt att få tillträde till en personuppgiftsansvarigs eller ett personuppgiftsbiträdes lokaler. Enligt vår bedömning kan en undersökning av lokalerna i de allra flesta fall ske med innehavarens medgivande. I vart fall torde risken för att tillsynsmyndigheten annars beslutar om tillfälligt förbud mot behandlingen, med stöd av artikel 58.2 f i dataskyddsförordningen, göra innehavaren tillräckligt benägen att ge tillsynsmyndigheten det tillträde den har rätt till enligt artikel 58.1 f. Detta gäller i synnerhet då en underlåtelse att rätta sig efter ett föreläggande eller att ge tillsynsmyndigheten tillgång till uppgifter kan medföra att administrativa sanktionsavgifter tas ut enligt artikel 83.5 e. Enligt uppgift från Datainspektionen har tvångsåtgärder hittills aldrig behövts och det finns enligt vår bedömning inget skäl att anta att det kommer att behövas när dataskyddsförordningen börjar tillämpas.

⁸ Prop. 1997/98:44 s. 101.

⁹ Prop. 1997/98:44 s. 102.

¹⁰ Se t.ex. 5 kap. 3 § konkurrenslagen (2008:579) och 45 kap. 13 § skatteförfarandelagen. Enligt lagen (2010:1010) om kreditvärderingsinstitut, som kompletterar Europaparlamentets och rådets förordning (EG) nr 1060/2009 av den 16 september 2009 om kreditvärderingsinstitut, krävs dock inte något domstolsbeslut för att tillsynsmyndigheten ska kunna utföra en platsundersökning utan medgivande, se prop. 2011/12:40 s. 23. Detsamma gäller även enligt exempelvis lagen (2013:287) med kompletterande bestämmelser till EU:s förordning om OTC-derivat, centrala motparter och transaktionsregister.

¹¹ Vad gäller bevissäkring enligt skatteförfarandelagen är det i stället Kronofogdemyndigheten eller granskningsledaren själv som verkställer förvaltningsrättens beslut, se 69 kap. 3 § skatteförfarandelagen.

I likhet med den bedömning som gjordes vid genomförandet av dataskyddsdirektivet anser vi därför att det inte behövs några bestämmelser som ger tillsynsmyndigheten möjlighet att tillgripa tvångsåtgärder för att genomföra en platsundersökning. Vi anser också att det vore olämpligt, med tanke på de integritetsrisker som ett sådant förfarande skulle kunna föranleda. Vi lämnar således i inga förslag i denna del.

Tillsynsmyndigheten får besluta om radering

I artikel 58.2 g i dataskyddsförordningen anges att tillsynsmyndigheten bland annat får förelägga om radering av personuppgifter enligt artikel 17. Den personuppgiftsansvarige är enligt den senare bestämmelsen skyldig att radera personuppgifter bland annat om personuppgifterna inte längre är nödvändiga för de ändamål för vilka de samlats in eller på annat sätt behandlats eller om personuppgifterna har behandlats på ett olagligt sätt.

Enligt 47 § PUL får beslut om utplåning endast fattas av förvaltningsrätten, på ansökan av tillsynsmyndigheten. Frågan är om ett föreläggande om radering enligt artikel 58.2 g i dataskyddsförordningen bör omfattas av en liknande skyddsåtgärd.

Ett föreläggande om radering av personuppgifter är onekligen en mycket ingripande åtgärd ur den personuppgiftsansvariges perspektiv. När raderingen väl har verkställts är åtgärden oåterkallelig. I det allmännas verksamhet kan radering i vissa fall också vara otillåten, om tillämplig gallringsföreskrift saknas. Om det senare skulle visa sig att raderingen var onödig eller felaktig kan den inte ångras. I vissa fall kan det till och med vara omöjligt att på nytt inhämta eller återskapa personuppgifterna.

Detta utgör dock inget skäl för att frånga principen om att prövningen av om en åtgärd ska vidtas ska göras av tillsynsmyndigheten som första instans. Tillsynsmyndighetens förelägganden kan överklagas med stöd av den bestämmelse om rätt att överklaga beslut som vi föreslår i avsnitt 19.7. Enligt vår bedömning saknas det därför skäl att föreskriva en särskild ordning, såsom krav på förhandstillstånd eller beslut av domstol, när tillsynsmyndigheten utövar sin befogenhet enligt artikel 58.2 g att förelägga om radering av personuppgifter. Vi lämnar därför inget sådant förslag.

Särskilt förfarande då förhandsbesked från EU-domstolen krävs

Tillsynsmyndigheten ska enligt artikel 58.5 i dataskyddsförordningen ha befogenhet att bland annat inleda eller på övrigt vis delta i rättsliga förfaranden, för att verkställa bestämmelserna i förordningen. En motsvarande bestämmelse finns i artikel 28.3 tredje strecksatsen i dataskyddsdirektivet, men berördes inte vid genomförandet av direktivet i svensk rätt.

I det mål som gällde giltigheten av kommissionens beslut att de så kallade Safe Harbor-principerna säkerställde ett adekvat skydd för överförda personuppgifter klargjorde EU-domstolen att bestämmelsen i dataskyddsdirektivet kan innebära ett krav på kompletterande processuella bestämmelser i nationell rätt.¹² I domen angavs att det ankommer på den nationella lagstiftaren att föreskriva rättsmedel som gör det möjligt för tillsynsmyndigheten att vid nationella domstolar göra gällande de invändningar mot behandlingen av personuppgifter som den anser att det finns fog för. På så sätt kan nationella domstolar, om de delar myndighetens tvivel angående en unionsrättsakts giltighet, hänskjuta en begäran om förhandsavgörande till EU-domstolen för att pröva rättsaktens giltighet. Bakgrunden till detta uttalande är att det bara är EU-domstolen som kan förklara en unionsrättsakt ogiltig. En nationell tillsynsmyndighet har inte denna befogenhet och måste därför tillämpa en unionsrättsakt, även om det finns skäl att ifrågasätta dess förenlighet med fördragen eller annan unionsrätt. Inte heller en nationell domstol kan ogiltigförklara en unionsrättsakt, men däremot kan domstolen begära förhandsavgörande från EU-domstolen och på så sätt få till stånd ett klargörande.

I svensk rätt finns det ingen möjlighet att väcka en renodlad lagprövningstalan i domstol. Det finns inte heller någon generell möjlighet för tillsynsmyndigheter att initiera en domstolsprövning enbart i syfte att skapa förutsättningar för ett klargörande från EU-domstolen. En sådan möjlighet bör dock enligt vår mening införas på dataskyddsområdet, för att Sverige fullt ut ska uppfylla kraven i artikel 58.5 i dataskyddsförordningen. Om det finns skäl att ifrågasätta om en unionsrättsakt som påverkar tillämpningen av dataskyddsförordningen är giltig, till exempel om ett kommissionsbeslut

¹² Dom Schrems, C-362/14, EU:C:2015:650, punkt 65. Se även Reichel, Nationella dataskyddsmyndigheter som lagprövare av EU-rätten, Förvaltningsrättslig tidskrift nr 1/16.

är förenligt med förordningen och fördragen, kan det vara olämpligt att tillsynsmyndigheten själv fattar beslut om åtgärder enligt artikel 58.2 i dataskyddsförordningen, såsom att den personuppgiftsansvarige ska föreläggas att radera personuppgifter eller att behandling av personuppgifter ska förbjudas. I en sådan situation bör tillsynsmyndigheten i stället kunna ansöka hos allmän förvaltningsdomstol om att åtgärden ska beslutas. Om domstolen i ett sådant mål delar tillsynsmyndighetens tvivel angående giltigheten av den unionsrättsakt som förhindrar eller kräver att åtgärden vidtas, kan domstolen begära ett förhandsavgörande från EU-domstolen och därigenom få rättsaktens giltighet prövad innan något beslut om åtgärden fattas.

Tillsynsmyndighetens ansökan bör göras hos den förvaltningsrätt som är behörig att pröva ett överklagande av tillsynsmyndighetens beslut. Prövningstillstånd bör krävas vid överklagande till kammarrätten. Denna typ av ansökningsförfarande hos domstol finns redan på ett flertal tillsynsområden, bland annat i 47 § PUL, och skulle därmed inte i sig utgöra något främmande element i svensk processrätt. På detta sätt kan således förordningens krav på rättsmedel för tillsynsmyndigheten uppfyllas, utan att något nytt processuellt institut behöver tillskapas.

19.6 Gemensamma tillsynsinsatser

19.6.1 Gällande rätt

Svensk grundlag

Vårt uppdrag i denna del är att bedöma om det bör införas bestämmelser som möjliggör en överföring av den svenska tillsynsmyndighetens befogenheter till en annan medlemsstats tillsynsmyndighet. Det finns därför anledning att redogöra för den svenska grundlagsregleringen på detta område.

Överlåtelse av beslutanderätt inom ramen för samarbetet i EU

Inom ramen för samarbetet i EU kan riksdagen överlåta beslutanderätt som inte rör principerna för statskicket (10 kap. 6 § regeringsformen). Sådan överlåtelse förutsätter att fri- och rättighetsskyddet inom det samarbetsområde till vilket överlåtelsen sker motsvarar det

som ges i regeringsformen och i den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna. Riksdagen kan besluta om sådan överlåtelse, om minst tre fjärdedelar av de röstande och mer än hälften av riksdagens ledamöter röstar för det. Riksdagens beslut kan också fattas i den ordning som gäller för stiftande av grundlag.

Den överlåtelse av beslutanderätt som har skett som en följd av Sveriges medlemskap i EU kommer till uttryck genom lagen med anledning av Sveriges anslutning till Europeiska unionen (anslutningslagen). I 2 § anslutningslagen föreskrivs att anslutningsfördraget och de grundläggande fördragen m.m. gäller här i landet med den verkan som följer av fördragen. Genom bestämmelsen införlivas hela det unionsrättsliga regelverket i den svenska rätten. I 3 § samma lag föreskrivs bland annat att EU får fatta beslut som gäller här i landet i den omfattning och med den verkan som följer av de fördrag och andra instrument som anges i 4 §. Det är genom den bestämmelsen som överlåtelsen av beslutanderätt till EU kommer till uttryck. I 4 § anslutningslagen finns en uppräkningslista av de fördrag och andra instrument som avses i 2 och 3 §§.

Systemet är uppbyggt så att riksdagen genom anslutningslagen en gång för alla beslutar om den överlåtelse av beslutsbefogenheter som respektive fördrag kräver. För varje nytt fördrag som har förutsatt överlåtelse av beslutsbefogenheter har alltså riksdagen dels godkänt det aktuella fördraget, dels beslutat om ändring av 4 § anslutningslagen, dvs. beslutat om införlivande och överlåtelse av beslutsbefogenheter. Detta innebär att det inte behövs någon ytterligare överlåtelse av beslutsbefogenheter till EU när t.ex. ett direktiv som har rättslig grund i fördragen ska införlivas i svensk lagstiftning; överlåtelsen har ju redan skett.¹³

Överlåtelse av rättsskipnings- eller förvaltningsuppgift

Regeringsformens bestämmelser om rättsskipning och förvaltning utgår från förutsättningen att dessa funktioner ska handhas av svenska organ. Rättsskipnings- eller förvaltningsuppgifter som inte direkt grundar sig på regeringsformen kan dock, även i andra fall än de som

¹³ Starrsjö, Regeringsform (1974:152) 10 kap. 6 §, Lexino 2016-01-23.

avses i 10 kap. 6 § regeringsformen, genom beslut av riksdagen överlåtas till en annan stat, till en mellanfolklig organisation eller till en utländsk eller internationell inrättning eller samfällighet (10 kap. 8 § regeringsformen). Riksdagen får i lag även bemyndiga regeringen eller någon annan myndighet att i särskilda fall besluta om en sådan överlåtelse. Om uppgiften innefattar myndighetsutövning, fattar riksdagen beslut om överlåtelse eller bemyndigande enligt den särskilda kvorumregeln i 10 kap. 6 § andra stycket regeringsformen, dvs. med kvalificerad majoritet, eller genom beslut av två riksdagar.

Den överlåtelse av beslutsbefogenheter som riksdagen har gjort enligt 10 kap. 6 § regeringsformen i samband med godkännande av nya EU-fördrag och ändring av anslutningslagen innebär att EU får fatta beslut som gäller här i landet i den omfattning och med den verkan som följer av fördragen. Om till exempel ett fullharmoniseringsdirektiv eller en förordning anger att medlemsstaternas tillsynsmyndigheter får tilldela befogenheter till andra medlemsstaters tillsynsmyndigheter krävs därmed inget ytterligare riksdagsbeslut om överlåtelse av beslutsbefogenheter. Riksdagen har redan överlåtit sin beslutsbefogenhet till unionslagstiftaren. Denne har i sin tur, genom den aktuella rättsakten, beslutat att tillsynsmyndigheterna får delegera sina befogenheter till andra medlemsstater. Något ytterligare riksdagsbeslut om överlåtelse av förvaltningsuppgift enligt 10 kap. 8 § regeringsformen krävs därmed inte i en sådan situation.¹⁴

19.6.2 Dataskyddsförordningen

Dataskyddsförordningen innehåller många och detaljerade bestämmelser om tillsynsmyndigheterna. Bland annat regleras tillsynsmyndigheternas uppgifter och befogenheter (artiklarna 57 och 58). Varje tillsynsmyndighet är behörig att utföra dessa uppgifter och utöva dessa befogenheter inom sin egen medlemsstats territorium (artikel 55.1). Vid gränsöverskridande personuppgiftsbehandling kommer det därmed att finnas flera behöriga tillsynsmyndigheter. I sådana situationer ska tillsynsmyndigheten för den personuppgiftsansvariges eller personuppgiftsbitrådets huvudsakliga eller enda verksamhetsställe vara behörig att agera som *ansvarig* tillsynsmyndighet (arti-

¹⁴ Jfr prop. 2011/12:175 s. 33 eller 2015/16:KU3y s. 3.

kel 56.1).¹⁵ Varje tillsynsmyndighet ska dock vara behörig att behandla klagomål som lämnats in till denna eller ärenden om överträdelser av förordningen, om sakfrågan i ärendet endast rör ett verksamhetsställe i medlemsstaten eller i väsentlig grad påverkar registrerade endast i medlemsstaten (artikel 56.2).

Den ansvariga tillsynsmyndigheten ska samarbeta med de andra berörda tillsynsmyndigheterna i en strävan att uppnå samförstånd, och tillsynsmyndigheterna ska utbyta all relevant information med varandra (artikel 60.1). Den ansvariga tillsynsmyndigheten får när som helst begära att andra berörda tillsynsmyndigheter ska ge ömsesidigt bistånd och får genomföra gemensamma insatser, i synnerhet för att utföra utredningar eller övervaka genomförandet av en åtgärd som avser en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad i en annan medlemsstat (artikel 60.2).

Tillsynsmyndigheterna ska vid behov genomföra gemensamma insatser, inbegripet gemensamma utredningar och gemensamma verkställighetsåtgärder (artikel 62.1). Om den personuppgiftsansvarige eller personuppgiftsbiträdet har verksamhetsställen i flera medlemsstater, eller om ett betydande antal registrerade personer i mer än en medlemsstat sannolikt kommer att påverkas i väsentlig grad av att uppgifter behandlas, ska tillsynsmyndigheterna i var och en av dessa medlemsstater ha rätt att delta i de gemensamma insatserna (artikel 62.2).

Vid gemensamma insatser kan de deltagande tillsynsmyndigheternas ledamöter och personal tilldelas befogenheter av värdlandets tillsynsmyndighet. Denna tillsynsmyndighet får också, i den mån den nationella lagstiftningen tillåter detta, medge att de deltagande tillsynsmyndigheternas ledamöter eller personal utövar de utredningsbefogenheter som de har enligt lagstiftningen i sin egen medlemsstat (artikel 62.3).

¹⁵ Artikel 56 ska dock enligt artikel 55.2 inte tillämpas om behandlingen utförs av myndigheter eller privata organ som agerar på grundval av artikel 6.1 c eller e. Då ska endast tillsynsmyndigheten i den berörda medlemsstaten vara behörig.

19.6.3 Överväganden

Utredningens bedömning: Den svenska tillsynsmyndigheten får, i enlighet med gällande svensk rätt, förordna företrädare för en utländsk myndighet att agera för tillsynsmyndighetens räkning.

Det bör för närvarande inte införas något bemyndigande som gör det möjligt för tillsynsmyndigheten att medge företrädare för en utländsk tillsynsmyndighet att inom svenskt territorium agera enligt den medlemsstatens lagstiftning.

Tilldelning av befogenheter enligt svensk rätt

Första meningen i artikel 62.3 i dataskyddsförordningen består av två bestämmelser. Enligt den första bestämmelsen får en tillsynsmyndighet tilldela befogenheter, även utredningsbefogenheter, till ledamöter eller personal från en annan medlemsstats tillsynsmyndighet som deltar i gemensamma insatser. Bestämmelsen innebär att företrädare för en utländsk tillsynsmyndighet kan ges befogenhet att utöva offentlig makt i Sverige, i enlighet med den lagstiftning som gäller för den svenska tillsynsmyndigheten. Detta är enligt vår mening inte detsamma som att en förvaltningsuppgift överläts till en utländsk tillsynsmyndighet. Av bestämmelsen framgår tvärtom tydligt att avsikten är att det är fysiska personer, ledamöter eller personal, som ska kunna tilldelas sådana befogenheter. Den svenska tillsynsmyndigheten kan således förordna företrädare för den andra myndigheten att utföra vissa uppgifter eller att inom ramen för vissa angivna befogenheter annars agera för tillsynsmyndighetens räkning. Enligt gällande svensk rätt är tillsynsmyndigheten fri att besluta om sådana förordnanden, även om det för anställning hade krävts svenskt medborgarskap. Några författningsåtgärder behövs därmed inte för att uppfylla denna del av bestämmelsen.

Enligt den sista meningen i artikel 62.3 ska en företrädare som tilldelas befogenheter omfattas av den medlemsstats nationella rätt som gäller för värdlandets tillsynsmyndighet. Det innebär bland annat att företrädaren omfattas av offentlighets- och sekretesslagens bestämmelser om tystnadsplikt och att denne kan ställas till ansvar för eventuella tjänstefel.

Medgivande att utöva befogenheter enligt utländsk rätt

Enligt den andra bestämmelsen i den första meningen i artikel 62.3 i dataskyddsförordningen får tillsynsmyndigheten medge företrädare för den deltagande myndigheten att utöva de utredningsbefogenheter som tilldelats dem enligt lagstiftningen i deras egen medlemsstat. I praktiken skulle ett sådant medgivande innebära att en utländsk tillsynsmyndighet får behörighet att agera på svenskt territorium i enlighet med utländsk lagstiftning. Medgivandet skulle därför enligt vår bedömning utgöra en överlåtelse av förvaltningsuppgift i regeringsformens mening. I bestämmelsen anges dock att medgivande får lämnas bara om lagstiftningen i värdlandet tillåter det. Tillsynsmyndigheterna har således inte direkt genom dataskyddsförordningen bemyndigats att medge andra medlemsstaters myndigheter rätt att utöva sina egna befogenheter inom värdlandets gränser. Det är i stället den nationella rätten i värdlandet som avgör om myndigheten överhuvudtaget kan vidta en sådan åtgärd.

En möjlighet för tillsynsmyndigheten att tillåta utländska myndighetsföreträdare att inom svenskt territorium utöva befogenheter enligt utländsk lagstiftning, bör enligt vår mening inte införas med mindre än att det finns ett tydligt och uttalat behov som inte kan uppfyllas på något annat sätt. Något sådant behov har inte framkommit. Det bör därför vara tillräckligt att den utländska myndigheten får delta i insatserna i enlighet med dataskyddsförordningens direkt tillämpliga bestämmelser. Det kan noteras att lagstiftaren har gjort liknande bedömningar i andra ärenden rörande gränsöverskridande tillsyn.¹⁶

19.7 Överklagande av tillsynsmyndighetens beslut

19.7.1 Gällande rätt

Enligt 22 § förvaltningslagen får ett beslut överklagas av den som beslutet angår, om det har gått honom emot och beslutet kan överklagas. I 22 a § samma lag anges att beslut överklagas hos allmän förvaltningsdomstol och att prövningstillstånd krävs vid överklagande till kammarrätten.

¹⁶ Se t.ex. prop. 2012/13:4 s. 47 eller prop. 2015/16:9 s. 191 f.

I 51 § PUL anges att tillsynsmyndighetens beslut om annat än föreskrifter får överklagas hos allmän förvaltningsdomstol. I samma paragraf anges att tillsynsmyndigheten får bestämma att dess beslut ska gälla även om det överklagas.

19.7.2 Dataskyddsförordningen

Som redan har nämnts ska utövandet av de befogenheter som tillsynsmyndigheten tilldelas enligt artikel 58 i dataskyddsförordningen omfattas av lämpliga skyddsåtgärder, inbegripet effektiva rättsmedel (artikel 58.4). I artikel 83.8 upprepas kravet på lämpliga skyddsåtgärder avseende tillsynsmyndighetens befogenheter att påföra administrativa sanktionsavgifter.

Enligt artikel 78.1 ska varje fysisk eller juridisk person ha rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut rörande dem som meddelats av en tillsynsmyndighet. I skälen anges att denna rätt även avser beslut om att avvisa eller avslå ett klagomål. Rätten till rättsmedel ska inte påverka något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol. Talan mot en tillsynsmyndighet ska enligt artikel 78.3 väckas vid domstolarna i den medlemsstat där tillsynsmyndigheten har sitt säte. Kravet på effektiva rättsmedel utvecklas i skäl 143 till förordningen.

19.7.3 Överväganden och förslag

Utredningens förslag: Tillsynsmyndighetens beslut enligt dataskyddsförordningen samt dess beslut om administrativa sanktionsavgifter enligt dataskyddslagen ska få överklagas till allmän förvaltningsdomstol. Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Tillsynsmyndighetens beslut att avslå en begäran om besked med anledning av ett klagomål ska få överklagas till allmän förvaltningsdomstol (dröjsmålstalan). Domstolens beslut ska inte kunna överklagas.

Den som beslutet gäller ska få överklaga

Rätten till ett effektivt rättsmedel enligt artikel 78.1 i dataskyddsförordningen avser rättsligt bindande beslut som meddelats av tillsynsmyndigheten. Rätten tillkommer varje fysisk eller juridisk person som beslutet rör. Däremot omfattas inte sådana åtgärder som inte är rättsligt bindande, såsom tillsynsmyndighetens yttranden eller rådgivning.

Rätten till ett effektivt rättsmedel mot myndighetsbeslut tillgodoses i svensk rätt normalt genom möjligheten att överklaga beslutet till allmän förvaltningsdomstol, dvs. till förvaltningsrätt som första instans. Detta bör gälla även här och uttryckligen anges i dataskyddslagen. Rätten att överklaga bör omfatta dels sådana beslut som tillsynsmyndigheten får meddela enligt dataskyddsförordningen, dels sådana beslut om administrativa sanktionsavgifter som får meddelas med stöd av dataskyddslagen. Övriga beslut som fattas av tillsynsmyndigheten enligt dataskyddslagen bör inte omfattas av den generella överklagandebestämmelsen. Liksom enligt personuppgiftslagen bör prövningstillstånd krävas vid överklagande av förvaltningsrättens beslut till kammarrätten.

Talerätt har enligt förvaltningslagen den som beslutet angår, om beslutet har gått denne emot. Den ordningen överensstämmer enligt vår bedömning med kravet på rättsmedel enligt artikel 78.1 i dataskyddsförordningen och bör således gälla även för beslut som tillsynsmyndigheten fattar enligt förordningen och den dataskyddslag som vi föreslår. I praktiken innebär detta i normalfallet att det är den som beslutet riktas mot, oftast en personuppgiftsansvarig, ett personuppgiftsbiträde eller ett certifieringsorgan, som har rätt att överklaga. Det kan dock inte uteslutas att ett beslut i något fall skulle kunna ha rättsligt bindande följder även för andra än den som beslutet riktas mot. Dessa skulle i så fall också ha rätt att överklaga beslutet, enligt förvaltningslagens generella bestämmelse om talerätt.

Enligt svensk rättspraxis rörande personuppgiftslagen är Datainspektionens beslut att inte vidta någon åtgärd med anledning av en anmälan eller att avskrika ett tillsynsärende inte överklagbart (se RÅ 2010 ref. 29). I skäl 143 till dataskyddsförordningen anges dock att tillsynsmyndighetens beslut att avvisa eller avslå ett klagomål ska kunna angripas med ett effektivt rättsmedel. Den som berörs av ett sådant beslut är den enskilde som har lämnat in klagomålet. Vidare

anges i artikel 77.2 att tillsynsmyndigheten ska underrätta den enskilde om hur arbetet fortskrider och vad resultatet blir, inbegripet möjligheten till rättslig prövning enligt artikel 78. EU-domstolen har angett att motsvarande bestämmelse i dataskyddsdirektivet (artikel 28.3) innebär att den person som har kommit in med en begäran till tillsynsmyndigheten ska ha tillgång till rättsmedel med vilka han eller hon vid nationella domstolar kan angripa det beslut som gått vederbörande emot.¹⁷ Dessa omständigheter skulle kunna tala för att dataskyddsförordningen förutsätter att den enskilde ska ha en generell rätt att överklaga tillsynsmyndighetens beslut att till exempel inte vidta någon åtgärd med anledning av ett klagomål.

Det finns emellertid också omständigheter som talar emot en sådan tolkning. Enligt artikel 78.1 är det den som beslutet rör som ska ha rätt till ett effektivt rättsmedel. Dessutom ska beslutet vara rättsligt bindande för denne. Ett beslut om att inte vidta några åtgärder med anledning av ett klagomål medför normalt inte några rättsligt bindande följder för den som har lämnat in klagomålet, även om det inte kan uteslutas att det någon gång skulle kunna förekomma, vilket i så fall skulle ge talerätt enligt förvaltningslagen. Dessutom skulle en ovillkorlig rätt till domstolsprövning av ett sådant beslut underminera tillsynsmyndighetens oberoende ställning, såsom denna kommer till uttryck i exempelvis artikel 52.1 i dataskyddsförordningen. Enligt artikel 57.1 f i dataskyddsförordningen ska tillsynsmyndigheten behandla klagomål och "där så är lämpligt" undersöka den sakfråga som klagomålet gäller. Tillsynsmyndigheten har därmed inte någon skyldighet att vidta tillsynsåtgärder eller ens att alltid närmare undersöka sakförhållandena. Tvärtom har tillsynsmyndigheten enligt dataskyddsförordningen, precis som enligt svensk tillsynstradition, ett uttalat utrymme för att själv avgöra vilka tillsynsärenden som ska drivas och på vilket sätt det ska ske. Det framgår inte heller uttryckligen av förordningen att tillsynsmyndigheten måste fatta ett formellt beslut i varje klagomåls- eller tillsynsärende.

Sammanfattningsvis anser vi att det är oklart om dataskyddsförordningen medför att den registrerade har rätt att överklaga tillsynsmyndighetens beslut att inte vidta någon åtgärd med anledning av ett klagomål. Oavsett hur förordningen ska tolkas i detta avseende, krävs det emellertid inte några författningsåtgärder i svensk rätt. Vi över-

¹⁷ Se t.ex. dom Schrems, C-362/14, EU:C:2015:650, punkt 64.

lämnar därför till domstolarna att, genom en unionskonform tolkning av förvaltningslagens generella talerättsbestämmelse, ta ställning i frågan.

Formerna för överklagande av tillsynsmyndighetens beslut, vilken överklagandefrist som ska gälla, talerätt m.m., bör inte avvika från förvaltningslagens bestämmelser. Vi föreslår därför inga särskilda bestämmelser om detta.

Den som har begärt besked om handläggningen av ett klagomål ska få överklaga ett beslut att avslå begäran (dröjsmålstan)

En registrerad som har lämnat in ett klagomål till tillsynsmyndigheten ska enligt dataskyddsförordningen ha rätt till ett effektivt rättsmedel, om myndigheten inte handlägger klagomålet eller tar lång tid på sig (artikel 78.2). I avsnitt 19.4 har vi därför föreslagit att tillsynsmyndigheten på skriftlig begäran av den registrerade ska vara skyldig att lämna besked om myndigheten avser att utöva tillsyn eller inte. Om myndigheten inte inom två veckor efter att begäran kom in kan lämna ett sådant besked, ska myndigheten i ett särskilt beslut avslå begäran om besked. Avsikten med detta är att den registrerade ska kunna få ett motiverat beslut rörande handläggningsfrågan som sedan kan överklagas till allmän förvaltningsdomstol. På så sätt kan den registrerade få till stånd en domstolsprövning av om handläggningstiden är rimlig. Om domstolen bifaller överklagandet ska domstolen förelägga tillsynsmyndigheten att inom en viss angiven tid lämna besked till den registrerade i frågan om tillsyn med anledning av klagomålet kommer att utövas. Domstolens beslut bör dock inte kunna överklagas till ytterligare en instans.

Som framgår av avsnitt 19.4 kan den registrerade komma in med en förnyad begäran om besked rörande handläggningen av ett klagomålsärende först tre månader efter det att tillsynsmyndigheten beslutat att avslå en första begäran om besked i ärendet. Om en sådan ny begäran kommer in innan denna tidsfrist har förflutit, ska alltså tillsynsmyndigheten inte göra någon prövning i sak utan i stället avvisa begäran. Ett sådant avvisningsbeslut bör inte vara överklagbart.

Redan i dag gäller skyndsamhetskrav och informationskyldighet enligt förvaltningslagens allmänna bestämmelser och eventuella brister i handläggningen kan anmälas till och bli föremål för prövning av JO. Såvitt vi känner till förekommer det i dag ingen utebliven eller

långsam handläggning av klagomål hos den svenska tillsynsmyndigheten. Det praktiska värdet av de bestämmelser rörande besked om handläggningen av ett klagomål och dröjsmålstalan som vi föreslår kan mot denna bakgrund ifrågasättas. I avsaknad av en generell reglering i förvaltningslagen om åtgärder vid dröjsmål bedömer vi dock att de föreslagna bestämmelserna behövs för att dataskyddsförordningens krav på effektiva rättsmedel ska anses uppfyllda. För det fall att riksdagen i enlighet med regeringens förslag beslutar om en ny förvaltningslag som innehåller generellt tillämpliga bestämmelser om åtgärder vid dröjsmål kan det dock finnas anledning att särskilt överväga om detta behov kvarstår.

Tillsynsmyndighetens beslut ska i vissa fall kunna verkställas innan det har vunnit laga kraft

Dataskyddsförordningen innehåller inga bestämmelser om när ett beslut som fattats av tillsynsmyndigheten ska börja gälla. Enligt vår mening finns det rättssäkerhetsskäl som talar för att huvudregeln bör vara att beslut inte ska kunna verkställas förrän överklagandetiden har löpt ut och beslutet vunnit laga kraft. I vissa fall måste dock åtgärder kunna vidtas snabbare än så.

I prop. 2016/17:180 med förslag till ny förvaltningslag föreslås generella bestämmelser om i vilka fall beslut kan verkställas innan överklagandetiden har gått ut (35 §). Bland annat föreslås att beslut som gäller endast tillfälligt, såsom tillfälliga förbud, ska kunna verkställas omedelbart. Vidare föreslås att en myndighet under vissa omständigheter ska få verkställa ett beslut omedelbart om ett väsentligt allmänt eller enskilt intresse kräver det. Enligt vår bedömning skulle dessa generella bestämmelser skapa en god balans mellan effektivitet och rättssäkerhet även när det gäller tillsynsmyndighetens beslut enligt dataskyddsförordningen. Vi lämnar därför inte något förslag i denna del. För det fall att regeringens förslag till ny förvaltningslag inte skulle komma att antas av riksdagen bör det dock övervägas om bestämmelser av motsvarande innebörd i stället bör tas in i dataskyddslagen.

19.8 Överklagande av andra beslut

19.8.1 Överväganden och förslag

Utredningens förslag: Datainspektionens beslut om att i enskilda fall tillåta andra än myndigheter att behandla personuppgifter som rör lagöverträdelse ska få överklagas till allmän förvaltningsdomstol. Detsamma gäller Riksarkivets förvaltningsbeslut om enskilda organs behandling av personuppgifter för arkivändamål av allmänt intresse. Prövningstillstånd ska krävas vid överklagande till kammarrätten.

I avsnitt 11.4 föreslår vi att Datainspektionen ska ges befogenhet att i enskilda fall fatta beslut om att andra än myndigheter får behandla personuppgifter som rör lagöverträdelse. De förvaltningsbeslut som Datainspektionen meddelar med stöd av den föreslagna bestämmelsen bör, av hänsyn till allmänna förvaltningsrättsliga principer, kunna överklagas till allmän förvaltningsdomstol. Prövningstillstånd bör krävas vid överklagande till kammarrätten.

Vidare föreslår vi i avsnitt 14.4 att Riksarkivet ska ges befogenhet att i enskilda fall få fastställa rättslig grund för ett enskilt organs behandling av personuppgifter för arkivändamål av allmänt intresse. På motsvarande sätt föreslås att Riksarkivet ska få fatta beslut som tillåter enskilda organ att behandla känsliga personuppgifter för sådana ändamål. Även sådana förvaltningsbeslut bör, av hänsyn till allmänna förvaltningsrättsliga principer, kunna överklagas till allmän förvaltningsdomstol. Prövningstillstånd bör krävas vid överklagande till kammarrätten.

Andra beslut enligt dataskyddslagen, såsom beslut om att meddela föreskrifter, bör inte kunna överklagas. Detta bör tydliggöras genom en uttrycklig bestämmelse i lagen.

19.9 Ideella organisationer som är verksamma inom dataskyddsområdet

19.9.1 Dataskyddsförordningen

Dataskyddsförordningen innehåller bestämmelser som tar sikte på organ, organisationer eller sammanslutningar som

- bedrivs utan vinstsyfte,
- är inrättade i enlighet med lagen i en medlemsstat,
- vars stadgeenliga mål är av allmänt intresse, och
- är verksamma inom området skydd av registrerades rättigheter och friheter när det gäller skyddet av deras personuppgifter.

Vi har, för enkelhetens skull, valt att benämna denna typ av sammanslutningar ideella organisationer.

Enligt artikel 80.1 ska den registrerade ha rätt att ge en sådan organisation i uppdrag att för hans eller hennes räkning lämna in ett klagomål till tillsynsmyndigheten enligt artikel 77 och att utöva den rätt till effektiva rättsmedel som avses i artiklarna 78 och 79. Den registrerade ska också, om så föreskrivs i medlemsstatens nationella rätt, ha rätt att ge den ideella organisationen i uppdrag att för hans eller hennes räkning utöva den rätt till ersättning som avses i artikel 82.

I artikel 80.2 anges att medlemsstaterna får föreskriva att en ideell organisation, oberoende av en registrerads mandat, har rätt att ge in klagomål till tillsynsmyndigheten enligt artikel 77 och utöva de rättigheter som avses i artiklarna 78 och 79. Organisationer får däremot inte ges rätt att kräva ersättning på en registrerad persons vägnar utan den registrerades mandat.

19.9.2 Överväganden

Utredningens bedömning: Den registrerade kan enligt gällande rätt ge en ideell organisation i uppdrag att företräda honom eller henne hos tillsynsmyndigheten. I allmän domstol och i förvaltningsdomstol kan endast fysiska personer agera ombud, men uppdraget att föra den registrerades talan kan ges till en företrädare för organisationen.

Ideella organisationer bör för närvarande inte ges rätt att utan den registrerades mandat föra talan i ärenden och mål om behandling av personuppgifter.

Dataskyddsförordningens tvingande bestämmelser avser inte att ge ideella organisationer talerätt i ärenden och mål om behandling av personuppgifter. Detta framgår tydligt genom att det i artikel 80.1 anges att den registrerade får ge en sådan organisation ”i uppdrag” att ”för hans eller hennes räkning” vidta vissa åtgärder. Ideella organisationer ska alltså kunna agera ombud för den registrerade i klagomålsärenden hos tillsynsmyndigheten, i mål om tillsynsmyndighetens dröjsmål och, om nationell rätt tillåter det, i mål om skadestånd. Frågan om huruvida det behövs kompletterande bestämmelser till dataskyddsförordningen rör sig därmed om möjligheten för sådana organisationer att vara ombud i förvaltningsärenden, mål i förvaltningsdomstol och mål i allmän domstol.

I artikel 80.2 däremot, ges medlemsstaterna en frivillig möjlighet att ge ideella organisationer talerätt, dvs. rätt att utan den registrerades mandat utöva dennes rättigheter. I den delen är frågan om en sådan ordning vore lämplig och önskvärd.

Ideella organisationer som ombud för den registrerade

Ideella organisationer kan, än så länge, företräda enskilda i förvaltningsärenden

I förvaltningsärenden får den enskilde enligt 9 § förvaltningslagen anlita ombud eller biträde, men ska medverka personligen, om myndigheten begär det. Visar ett ombud eller biträde oskicklighet eller oförstånd eller är han olämplig på något annat sätt, får myndigheten avvisa honom som ombud eller biträde i ärendet. I förarbetena till förvaltningslagen anges att reglerna inte innebär något hinder mot att juridisk person fungerar som ombud.¹⁸ Förvaltningslagen ställer inte heller upp några principiella krav eller begränsningar avseende ombudets kvalifikationer eller dennes relation till huvudmannen. I propositionen om ny förvaltningslag, prop. 2016/17:180, föreslås dock

¹⁸ Prop. 1971:30 del 2 s. 362.

bestämmelser som förhindrar juridiska personer att agera ombud i förvaltningsärenden (14 §).

Det finns därmed enligt gällande rätt möjlighet för den enskilde att ge en ideell organisation i uppdrag att för hans eller hennes räkning lämna in klagomål till tillsynsmyndigheten. Detsamma gäller vid utövande av rätten att hos Justitiekanslern begära skadestånd, när en personuppgiftsansvarig statlig myndighet har åsamkat den enskilde skada genom överträdelse av dataskyddsförordningen. Denna möjlighet kommer dock att försvinna om riksdagen antar förslaget om ny förvaltningslag.

En juridisk person kan inte vara ombud i domstol

Det förhåller sig emellertid annorlunda, enligt gällande rätt, när det gäller möjligheten för en juridisk person såsom en ideell organisation att företräda en enskild i domstol, dvs. i ett förvaltningsmål rörande tillsynsmyndighetens dröjsmål eller i ett skadeståndsmål i allmän domstol. Bestämmelserna om rättegångsombud i 12 kap. rättegångsbalken utgår nämligen från förutsättningen att ombudet är en fysisk person. En ideell organisation skulle därmed sannolikt avvisas som ombud i ett skadeståndsmål i allmän domstol. Detsamma gäller sedan den 1 juli 2013 även i mål i allmän förvaltningsdomstol. Bestämmelser om ombud finns bland annat i 48 och 49 §§ förvaltningsprocesslagen (1971:291) och av förarbetena till den nuvarande lydelsen framgår att det inte längre kommer att vara möjligt att i allmän förvaltningsdomstol använda sig av juridiska personer som ombud eller biträden.¹⁹

En företrädare för en ideell organisation kan dock företräda den enskilde, både i förvaltningsärenden och i domstol

Ett rättegångsombud ska enligt 12 kap. 2 § rättegångsbalken vara lämplig med hänsyn till redbarhet, insikter och tidigare verksamhet. I 48 § förvaltningsprocesslagen anges endast att ombudet ska vara lämpligt för uppdraget. Det finns varken i rättegångsbalken eller i förvaltningsprocesslagen, eller i förslaget till ny förvaltningslag, något

¹⁹ Prop. 2012/13:45 s. 106 f.

krav på att ombudet ska vara advokat eller jurist. Den företrädare för den ideella organisationen som skulle ha fört talan om organisationen själv hade godkänts som rättegångsombud skulle därmed normalt godkännas som ombud för den registrerade.²⁰

I förarbetena till 2013 års ändring av förvaltningsprocesslagen anges att ett uppdrag som ombud eller biträde i domstol bör vara förordat med ett personligt uppdrags- och ansvarsförhållande.²¹ Vi instämmer i denna bedömning. Även om en ideell organisation skulle få anlitas som ombud skulle det i realiteten vara en fysisk person som för den enskildes talan. Fullmakten till organisationen kan därmed utan olägenhet utformas så att den också omfattar den fysiska personen som faktiskt utför uppdraget. Mot denna bakgrund anser vi att det saknas skäl att föreslå några bestämmelser som avviker från rättegångsbalken och förvaltningsprocesslagen.

Ideella organisationer ska inte ges talerätt

Medlemsstaterna får enligt dataskyddsförordningen meddela nationella föreskrifter som ger ideella organisationer en självständig talerätt avseende registrerades rättigheter. En sådan talerätt skulle ge dessa organisationer möjlighet att utan den registrerades mandat ge in klagomål till tillsynsmyndigheten samt föra talan mot myndigheten om dess dröjsmål, om organisationen anser att den registrerades rättigheter har kränkts.

En liknande ordning gäller enligt svensk rätt i fråga om kränkningar i form av diskriminering. Enligt 6 kap. 2 § diskrimineringslagen får en ideell förening som enligt sina stadgar har att ta till vara sina medlemmars intressen och som inte är en arbetstagarorganisation, som part föra talan om diskriminering. En förutsättning är dock att den enskilde medger detta. Ett annat exempel som kan nämnas är möjligheten till organisationstalan enligt lagen (2002:599) om grupprättegång. I 5 § i den lagen anges att organisationstalan får väckas av en ideell förening som i enlighet med sina stadgar tillvaratar konsument- eller löntagarintressen i tvister mellan konsumenter och en

²⁰ Jfr prop. 2002/03:65 s. 167.

²¹ Prop. 2012/13:45 s. 106 f.

näringsidkare om någon vara, tjänst eller annan nytthet som näringsidkaren erbjuder till konsumenter.

När det gäller skyddet för den personliga integriteten har det under senare år börjat bli vanligare med ideella organisationer som är verksamma inom dataskyddsområdet. I Sverige är dock denna typ av verksamhet än så länge liten. Mot denna bakgrund, och då det inom ramen för vår utredning inte finns möjlighet att närmare analysera behovet av talerätt för sådana organisationer och vilka konsekvenser det i så fall skulle få, lämnar vi inget sådant förslag. Beroende på hur den ideella sektorn utvecklas är det dock inte uteslutet att det i framtiden kan komma att finnas skäl att utreda denna fråga särskilt.

19.10 Parallella domstolsförfaranden

19.10.1 Dataskyddsförordningen

Om en behörig domstol i en medlemsstat har information om att ett förfarande pågår i en domstol i en annan medlemsstat, rörande samma sakfråga och samma personuppgiftsansvarig eller personuppgiftsbiträde, ska den förstnämnda domstolen enligt artikel 81.1 i dataskyddsförordningen kontakta den andra domstolen för att få det bekräftat.

I artikel 81.2 anges att om förfaranden som rör samma sakfråga och samma personuppgiftsansvarig eller personuppgiftsbiträde pågår i en domstol i en annan medlemsstat, får alla andra behöriga domstolar än den där förfarandet först inleddes vilandeförklara förfarandena. Om ett förfarande prövas i första instans får domstolen, utom den domstol vid vilken förfarandena först inleddes, enligt artikel 81.3 förklara sig obehörig på begäran av en av parterna. Detta gäller under förutsättningen att den domstol vid vilken förfarandet först inleddes är behörig att pröva de berörda förfarandena och dess lagstiftning tillåter förening av dessa.

I skäl 144 till förordningen anges att förfarandena ska anses vara relaterade, om de är så nära förenade att en gemensam handläggning och dom är påkallad för att undvika att oförenliga domar meddelas.

19.10.2 Överväganden

Utredningens bedömning: En svensk domstol kan förklara ett mål vilande, om ett förfarande rörande samma sakfråga pågår i en domstol i en annan medlemsstat. Däremot kan domstolen inte förklara sig obehörig att handlägga målet.

Domstolen kan förklara ett mål vilande

I 32 kap. 5 § rättegångsbalken finns en bestämmelse som innebär att rätten får förklara ett mål vilande, om det för prövning av målet är av synnerlig vikt att en fråga som är föremål för annan rättegång eller behandling i annan ordning först avgörs. Någon motsvarighet till denna bestämmelse finns inte i förvaltningsprocesslagen. Det innebär dock inte att förvaltningsdomstolar är förhindrade att förklara ett mål vilande av motsvarande skäl. Vid införandet av förvaltningsprocesslagen ansågs detta tvärtom så självklart att lagtexten inte behövde belastas med någon hänvisning till rättegångsbalken.²² Möjligheten till vilandeförklaring har inte bara utnyttjats när flera relaterade mål förekommit i samma domstol eller i olika svenska domstolar, utan har också använts för att invänta EU-domstolens dom i ett annat mål avseende en för målet central rättsfråga.²³

Sedan den 1 juli 2013 får Högsta förvaltningsdomstolen enligt 36 a § förvaltningsprocesslagen meddela prövningstillstånd som begränsas till att gälla en viss fråga eller en viss del av målet. I avvaktan på att prövning sker i enlighet med ett sådant begränsat prövningstillstånd får Högsta förvaltningsdomstolen förklara frågan om meddelande av prövningstillstånd rörande målet i övrigt helt eller delvis vilande. Med anledning av ett påpekande under remissbehandlingen från Högsta förvaltningsdomstolens ledamöter underströks i förarbetena att den omständigheten att denna typ av vilandeförklaring numera uttryckligen regleras i förvaltningsprocesslagen inte inskränker allmän förvaltningsdomstols möjligheter att även i andra sammanhang vilandeförklara mål.²⁴

²² Prop. 1971:30 del 2 s. 600.

²³ Se t.ex. RÅ 2005 ref. 33 och Kammarrättens i Stockholm dom den 22 augusti 2014 i mål nr 1724-13.

²⁴ Prop. 2012/13:45 s. 139.

Mot bakgrund av att förvaltningsdomstolarna redan på grundval av förvaltningsprocessrättsliga principer och praxis kan förklara mål vilande när ett mål rörande samma sakfråga pågår i en annan domstol, även en utländsk sådan, finns det enligt vår bedömning inget skäl att införa några särskilda bestämmelser i svensk rätt med anledning av artikel 81.2 i dataskyddsförordningen. Hur sådana situationer ska hanteras i praktiken får lämnas till domstolarna att avgöra.²⁵

Domstolen kan inte förklara sig obehörig

Om förfaranden som rör samma sakfråga pågår i flera domstolar, får varje domstol utom den där förfarandet först inleddes förklara sig obehörig på begäran av en av parterna (artikel 81.1). Detta förutsätter dock dels att den domstol där förfarandet först inleddes är behörig att göra prövningen, dels att dess lagstiftning tillåter förening av förfarandena.

Enligt 7 § förvaltningsprocesslagen kan ett mål överlämnas till en annan domstol om domstolen finner att den saknar behörighet att handlägga målet men att en annan motsvarande domstol skulle vara behörig. Vidare följer det av 8 a och 14 §§ lagen (1972:289) om allmänna förvaltningsdomstolar att mål under vissa omständigheter kan överlämnas, om det vid mer än en förvaltningsrätt eller kammarrätt förekommer mål som har nära samband med varandra. Det finns där- emot för närvarande inte några bestämmelser i svensk förvaltningsprocessrätt som möjliggör för en domstol att förklara sig obehörig att handlägga ett mål på den grunden att det vid en utländsk domstol förekommer ett mål som rör samma sakfråga. En svensk domstol skulle därmed inte kunna överlämna ett mål till en utländsk domstol i den situation som beskrivs i artikel 81.1 i dataskyddsförordningen och samtidigt förklara sig obehörig att handlägga målet. I bestämmelsen anges dock endast att domstolen "får" förklara sig obehörig. Förordningen är således i detta avseende inte tvingande och det finns därmed inte någon skyldighet för medlemsstaterna att införa processrättsliga bestämmelser som möjliggör ett sådant överlämnade. Vi ser därför inte något skäl att lämna ett förslag i denna del.

²⁵ Jfr prop. 2011/12:70 s. 68.

20 Ikraftträdande- och övergångsbestämmelser

20.1 Vårt uppdrag

I våra direktiv förutsätts att personuppgiftslagen måste upphävas redan i samband med att dataskyddsförordningen börjar tillämpas. Regeringen anser därför att det kan finnas behov av övergångsbestämmelser som i första hand innebär att lagen under en övergångsperiod fortsätter att gälla för sådan personuppgiftsbehandling som inte täcks av förordningens tillämpningsområde.

20.2 Ikraftträdande- och övergångsbestämmelser i förordningen

Av förordningens artikel 99.1 följer att förordningen träder i kraft den tjugonde dagen efter det att den har offentliggjorts i Europeiska unionens officiella tidning, vilket skedde den 4 maj 2016.

Av artikel 99.2 följer att förordningen ska tillämpas från och med den 25 maj 2018. I artikel 94 anges vidare att dataskyddsdirektivet ska upphöra att gälla med verkan från och med samma dag och att hänvisningar till det upphävda direktivet ska anses som hänvisningar till förordningen.

I skäl 171 anges att behandling som redan pågår den dag då förordningen börjar tillämpas bör bringas i överensstämmelse med förordningen inom en period av två år från det att förordningen träder i kraft. Om behandlingen grundar sig på samtycke enligt dataskyddsdirektivet anges vidare att det inte är nödvändigt att den registrerade på nytt ger sitt samtycke för att den personuppgiftsansvarige ska kunna fortsätta med behandlingen i fråga efter det att förordningen börjar tillämpas, om det sätt på vilket samtycket gavs överensstäm-

mer med villkoren i denna förordning. Beslut av kommissionen som antagits och tillstånd från tillsynsmyndigheterna som utfärdats på grundval av dataskyddsdirektivet ska enligt samma skäl vara fortsatt giltiga tills de ändras, ersätts eller upphävs.

I artiklarna 95 och 96 finns vissa bestämmelser av övergångskaraktär när det gäller förhållandet till direktiv 2002/58/EG om integritet och elektronisk kommunikation samt internationella avtal.

20.3 Överväganden och förslag

Utredningens förslag: Dataskyddslagen ska träda i kraft den 25 maj 2018, samtidigt som personuppgiftslagen ska upphöra att gälla. Personuppgiftslagen ska dock fortfarande gälla i den utsträckning som det i en annan lag eller förordning finns bestämmelser som innehåller hänvisningar till den.

Äldre föreskrifter, dvs. personuppgiftslagen, personuppgiftsförordningen och föreskrifter som har meddelats med stöd av dessa, ska fortfarande gälla för ärenden som har inletts hos Datainspektionen men inte avgjorts före ikraftträdandet. Äldre föreskrifter ska också gälla för överklagande av beslut som har meddelats med stöd av dessa föreskrifter liksom för överträdelser som har skett före ikraftträdandet.

Bestämmelserna om skadestånd i personuppgiftslagen ska gälla för skada som har orsakats före ikraftträdandet.

Utredningens bedömning: Någon övergångsbestämmelse som rör personuppgiftsbehandling som inte täcks av förordningens tillämpningsområde behöver inte införas.

Ikraftträdande

Enligt dataskyddsförordningens artikel 99 ska förordningen tillämpas från och med den 25 maj 2018. Vi föreslår därför att den nya lagen med kompletterande bestämmelser till förordningen ska träda ikraft den dagen. Samtidigt bör personuppgiftslagen upphöra att gälla (avsnitt 5.2.1).

Personuppgiftsbehandling utanför förordningens tillämpningsområde

När det gäller behandling av personuppgifter utanför förordningens tillämpningsområde innebär vårt förslag i avsnitt 6.4 att dataskyddsförordningen i den ursprungliga lydelsen samt dataskyddslagen ska tillämpas vid behandling av personuppgifter även i verksamhet som faller utanför förordningens tillämpningsområde enligt artikel 2.2 a och b. Förutsatt att denna del av våra förslag genomförs ser vi inget behov av någon särskild övergångsbestämmelse för sådan behandling.

Befintliga hänvisningar

Hänvisningar till personuppgiftslagen förekommer i ett stort antal sektorsspecifika författningar. Eftersom dataskyddsförordningen är direkt tillämplig från och med den 25 maj 2018 och personuppgiftslagen samtidigt kommer att upphävas är det naturligtvis av stor betydelse att de hänvisningar som finns i gällande författningar till den nuvarande personuppgiftslagen så snart som möjligt ändras och anpassas till dataskyddslagen och förordningen. Ett omfattande översynsarbete pågår just nu i utredningar och inom Regeringskansliet, men arbetet med att se över de följdändringar som kan behövas i både lag och förordning kommer att bli omfattande och ta tid. Vi bedömer därför att någon form av övergångsreglering när det gäller befintliga hänvisningar till personuppgiftslagen behövs.

En övergångsreglering som innebär att befintliga hänvisningar i stället ska avse förordningens och dataskyddslagens bestämmelser bedömer vi inte som möjlig eftersom regleringen skiljer sig för mycket åt i sak. För att undvika osäkerhet med brister i integritetsskyddet som följd talar, enligt vår mening, övervägande skäl för att låta den nuvarande personuppgiftslagen övergångsvis fortsätta att gälla i den utsträckning som det fortfarande finns hänvisningar kvar till den lagen. Som framhålls ovan bör självklart befintlig reglering skyndsamt anpassas till förordningen och dataskyddslagen.

Ärendehandläggning och överklagande av beslut

En utgångspunkt i förordningen är som nämnts att behandling som pågår den dag då förordningen börjar tillämpas ska ha bringats i överensstämmelse med förordningen när förordningen börjar tillämpas den 25 maj 2018. Personuppgiftsansvariga och personuppgiftsbiträden får därför förutsättas ha ordnat sin behandling så att exempelvis en begäran om information från en registrerad som inkommit men inte hunnit besvaras före den 25 maj 2018 kan tillmötesgå i enlighet med förordningens bestämmelser. Även tillsynsmyndighetens verksamhet bör i möjligaste mån ha anpassats till förordningens regelverk vid denna tidpunkt. Tillsynsärenden kan dock pågå under en längre tid och det är inte självklart att tillsynsmyndigheten helt kan styra över när underlaget är så fullständigt att beslut i ärendet kan fattas. Förelägganden om exempelvis säkerhetsåtgärder eller radering kan inte baseras på förordningens bestämmelser innan dessa är tillämpliga, utan måste utformas i enlighet med personuppgiftslagen fram till dess att förordningen börjar tillämpas. Det är lämpligt att sådana ärenden handläggs enligt personuppgiftslagen till dess de är avgjorda.

Vi ser därför ett behov av en övergångsbestämmelse som tydliggör att ärenden som har inletts hos Datainspektionen – genom att de anhängiggjorts av myndigheter eller enskilda, eller på inspektionens eget initiativ – före ikraftträdandet av dataskyddslagen men som vid den tidpunkten ännu inte har avgjorts, ska handläggas enligt personuppgiftslagen och föreskrifter som meddelats med stöd av den lagen. Detsamma bör gälla för överklagande av beslut som har meddelats med stöd av äldre föreskrifter.

Skadestånd

I 48 § PUL finns bestämmelser om skadeståndsskyldighet för personuppgiftsansvariga och möjlighet att jämka sådan ersättningsskyldighet i vissa fall. Dessa bestämmelser bör fortsätta att gälla för skada som har orsakats före upphävandet av personuppgiftslagen. I svensk rätt har det ansetts att det följer av allmänna rättsgrundsatser att nya skadeståndsbestämmelser blir tillämpliga i fråga om skadestånd till följd av skadefall som inträffar efter ikraftträdandet, och att det inte

behöver regleras i särskilda övergångsbestämmelser.¹ Avsaknad av en övergångsbestämmelse i detta avseende riskerar dock att orsaka osäkerhet om förhållandet mellan dataskyddsförordningens och personuppgiftslagens bestämmelser om skadestånd. Det förhållandet att ett stort antal sektorspecifika författningar innehåller hänvisningar till 48 § PUL gör också att det är lämpligt med en så tydlig reglering som möjligt. Vi menar mot denna bakgrund att det bör införas en särskild övergångsbestämmelse om detta.

Straffbestämmelsens avskaffande

Eftersom vårt förslag innebär att den straffrättsliga regleringen upphävs och i praktiken ersätts med en administrativ sanktionsavgift, uppkommer frågan om vad som ska gälla för straffbelagda gärningar som har begåtts vid behandling som upphört före den 25 maj 2018 men där överträdelsen inte lagförts innan de nya reglerna ska börja tillämpas.

Vid bedömningen av behovet att meddela övergångsbestämmelser för den nu nämnda situationen behöver bestämmelserna i såväl 2 kap. 10 § regeringsformen som 5 § andra stycket lagen (1964:163) om införande av brottsbalken beaktas.

I 2 kap. 10 § regeringsformen finns ett förbud mot retroaktiv straff- och skattelagstiftning. Förbudet mot retroaktiv skattelag anses analogivis tillämpligt beträffande straffliknande administrativa påföljder.² Att ta ut sanktionsavgifter för överträdelser som begåtts före den 25 maj 2018 skulle således strida mot retroaktivitetsförbudet.

Av 5 § andra stycket lagen om införande av brottsbalken framgår att straff ska bestämmas enligt den lag som gällde när gärningen företogs. Detta är dock inte fallet om annan lag gäller när dom meddelas, under förutsättning att den nya lagen leder till frihet från straff eller till lindrigare straff. Denna bestämmelse har enligt förarbetena generell räckvidd, dvs. den gäller även utanför brottsbalkens tillämpningsområde.³ Bestämmelsen ger uttryck för den lindrigaste lagens princip.

Bestämmelserna i dataskyddsförordningen och dataskyddslagen innebär att överträdelser mot den gällande dataskyddsregleringen överförs från det straffrättsliga området till ett system med enbart

¹ Prop. 1972:5 s. 593.

² Prop. 1975/76:209 s. 125.

³ Prop. 1964:10 s. 99.

administrativa sanktionsavgifter. Formellt sett får sanktionsavgiften anses lindrigare och borde därmed få genomslag bakåt i tiden. I prop. 2007/08:107, Administrativa sanktioner på yrkesfiskets område, föreslogs motsvarande ändringar beträffande sanktionssystemet. Lagrådet anförde i sitt yttrande över lagförslaget att om avsikten med lagändringarna inte var ägnade att ändra synen på vad som var straffbart utan önskemålet i stället var att skapa en annan och mer effektiv sanktionsform, faller motiven för en tillämpning av den lindrigaste lagens princip bort.⁴

När det gäller dataskyddsförordningens och dataskyddslagens system med kraftfulla sanktionsavgifter torde detta i många fall anses som en svårare sanktion än exempelvis ett bötesstraff enligt regleringen i personuppgiftslagen. Huvudsyftet med att överträdelse mot dataskyddsregleringen föreslås avkriminaliseras är framför allt effektivisering, och ska inte ses som ett uttryck för att överträdelserna ska bedömas lindrigare än tidigare. Vi menar därför att lindrigaste lagens princip inte gör sig gällande i detta fall. Äldre bestämmelser bör därför tillämpas på överträdelser som skett före dataskyddslagens ikraftträdande.

Tillsynsåtgärder

Det följer av allmänna principer och i någon mån av förordningens skäl 171 att förelägganden och förbud som har meddelats av tillsynsmyndigheten med stöd av personuppgiftslagen fortsätter att gälla efter upphävandet av den lagen. Det behövs därför inte någon särskild övergångsbestämmelse i den delen.⁵ Inte heller i övrigt finns det behov av ytterligare övergångsbestämmelser med anledning av personuppgiftslagens upphävande.

⁴ Prop. 2007/08:107 s. 66.

⁵ Prop. 2015/16:72 s. 56.

21 Konsekvenser

21.1 Vårt uppdrag

Kommittéförordningen

En utredning ska enligt kommittéförordningen (1998:1474) redovisa vilka konsekvenser förslagen i ett betänkande kan få i olika avseenden. I 14–15 a §§ föreskrivs bland annat att för det fall förslagen i ett betänkande påverkar kostnaderna eller intäkterna för staten, kommuner, landsting, företag eller andra enskilda, ska en beräkning av dessa konsekvenser redovisas i betänkandet. Om förslagen innebär samhällsekonomiska konsekvenser i övrigt så ska dessa redovisas. Vidare ska eventuella konsekvenser för den kommunala självstyrelsen, för brottsligheten och det brottsförebyggande arbetet, samt för bland annat sysselsättning och offentlig service i olika delar av landet redovisas. Detsamma gäller små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företag och för jämställdheten mellan kvinnor och män.

Våra direktiv

Regeringen ska enligt 16 § kommittéförordningen ange närmare i utredningsuppdraget vilka konsekvensbeskrivningar som ska finnas i ett betänkande. Enligt våra direktiv ska vi bedöma de ekonomiska konsekvenserna av förslagen för det allmänna och för enskilda. Det är alltså konsekvenserna av våra förslag till dataskyddslag med tillhörande förordning samt förslagen till ändringar i offentlighets- och sekretesslagen och arkivförordningen som vi har att bedöma enligt direktiven. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska vi föreslå hur dessa ska finansieras. Vi ska särskilt ange konsekvenser för företagen i form av kostnader och ökade admi-

nistrativa bördor. Vi ska också redovisa förslagets konsekvenser för den personliga integriteten.

Konsekvenser utanför vårt uppdrag

Det står klart att dataskyddsförordningens direkt tillämpliga bestämmelser kommer att leda till konsekvenser, både för det allmänna och för enskilda i Sverige. Förordningens bestämmelser kan bland annat förväntas öka kostnaderna för myndigheter och enskilda som är personuppgiftsansvariga eller personuppgiftsbiträden, i form av ökad administration och ökade kostnader initialt för anpassning av befintliga it-system. Det kommer särskilt initialt att krävas ökade resurser till utbildningsinsatser och eventuellt nyrekryteringar till tjänster som dataskyddsombud både för det allmänna och i den privata sektorn. Konsekvenserna av dataskyddsförordningens direkt tillämpliga bestämmelser ankommer dock inte på oss att bedöma.

Det bör noteras att dataskyddsförordningens konsekvenser för tillsynsmyndigheten tidigare har övervägts av Utredningen om tillsynen över den personliga integriteten. Den utredningen konstaterade i sitt betänkande (SOU 2016:65) att ytterligare resurser kommer att behöva tillföras, men att en slutgiltig uppskattning av resursbehovet kommer att behöva göras när de utredningar har slutförts som har i uppdrag att överväga dataskyddsförordningens och det nya dataskyddsdirektivets konsekvenser för hur tillsynen ska vara utformad.

Det bör slutligen påpekas att flertalet nationella bestämmelser som kompletterar dataskyddsförordningen kommer att finnas i sådan sektorsspecifik reglering som ligger utanför vårt uppdrag. För närvarande arbetar ett stort antal utredningar med anpassningar av nationell rätt med anledning av dataskyddsförordningen och det nya dataskyddsdirektivet. Konsekvenserna av deras förslag analyseras inom ramen för respektive utredning.

21.2 Förändringar som följer av våra förslag

Under respektive avsnitt i betänkandet görs för varje del överväganden avseende dataskyddsförordningens krav, utrymmet för nationell reglering och skäl som talar för och emot olika författningstekniska lösningar. I de övervägandena har vi exempelvis beaktat hur olika

lösningar skulle påverka den personliga integriteten och motstående intressen samt vilka effekter de skulle få för myndigheternas verksamhet. För en analys av konsekvenserna av andra möjliga lösningar än de vi föreslår hänvisas därför till dessa avsnitt.

En allmän utgångspunkt för vårt uppdrag har varit att sträva efter lösningar som ansluter till nuvarande systematik i personuppgiftslagen och personuppgiftsförordningen. De flesta bestämmelserna i dataskyddslagen och den kompletterande förordning som vi föreslår motsvarar i linje med detta i stort sett de nuvarande reglerna i personuppgiftslagen och personuppgiftsförordningen.

Vissa förslag innebär dock förändringar jämfört med den ordning som gäller i dag, och medför att en konsekvensanalys måste genomföras. Det gäller främst förslagen i avsnitt 14 om arkiv och statistik, i avsnitt 18 om sanktioner och i avsnitt 19 om processuella frågor.

Riksarkivet föreslås i avsnitt 14 få nya uppgifter i form av föreskriftsrätt och befogenhet att fatta beslut i enskilda fall när det gäller enskilda organs behandling av personuppgifter för arkivändamål av allmänt intresse.

I avsnitt 18 föreslås att sanktionsavgifter ska kunna beslutas även mot myndigheter. Denna arbetsuppgift för tillsynsmyndigheten är inte direkt föranledd av dataskyddsförordningens bestämmelser. I avsnittet bedöms vidare att någon straffbestämmelse motsvarande den som finns i personuppgiftslagen inte bör införas i dataskyddslagen.

Andra nyheter, som behandlas i avsnitt 19, är möjligheten för enskilda att i vissa fall begära besked från tillsynsmyndigheten om myndigheten avser att utöva tillsyn och att föra dröjsmålstalan mot ett sådant beslut. Det inrättas också en möjlighet för tillsynsmyndigheten att under vissa speciella omständigheter väcka talan i domstol. Övriga förslag beträffande rättsmedel i kapitel 19 motsvarar emellertid i allt väsentligt det som gäller i dag.

21.3 Ekonomiska konsekvenser

21.3.1 Ekonomiska konsekvenser för det allmänna

Utredningens bedömning: Förslagen kommer att innebära att Riksarkivet, Datainspektionen och de allmänna förvaltningsdomstolarna får något fler arbetsuppgifter, men kostnadsökningarna kommer inte att bli större än att de ryms inom de befintliga anslagen.

De konsekvenser som beskrivs nedan avser som nämnts tidigare enbart våra förslag och inte dataskyddsförordningens bestämmelser i stort. Vår analys utgår här från de förändringar som våra förslag medför jämfört med vad som gäller enligt nuvarande generella reglering, dvs. framför allt enligt personuppgiftslagen och personuppgiftsförordningen.

Förslagen medför att Riksarkivet får föreskriftsrätt och en rätt att besluta i vissa enskilda fall som myndigheten inte haft tidigare. Initialt kan detta förväntas leda till en något ökad arbetsbörda, men torde därefter inte kräva några ökade resurser. Vi bedömer inte att våra förslag innebär att Riksarkivet behöver tillskjutas medel utöver befintliga anslag.

Förslagen medför även nya arbetsuppgifter för Datainspektionen och de allmänna förvaltningsdomstolarna. Möjligheten att begära besked från Datainspektionen om handläggningen av ett inkommet klagomål kommer initialt att kräva att resurser läggs på utarbetande av rutiner för hur information om handläggningen ska lämnas till den registrerade liksom för hur framställningar om besked från registrerade ska hanteras. Eftersom det kan antas att Datainspektionen i de flesta fall kommer att ha behandlat ett klagomål inom tre månader på det sätt som förutsätts i dataskyddsförordningen, bedömer vi att de nya arbetsuppgifterna i förlängningen inte kräver några mer omfattande resurser.

Vi bedömer att en dröjsmålstalan inte kommer väckas i domstol i mer än ett fåtal fall varje år. Målen är dessutom av enkel beskaffenhet och torde därför kunna avgöras av en ensamdomare. Mot den bakgrunden bör inte heller domstolens resurser behöva tas i anspråk i någon större utsträckning för denna måltyp.

Vad gäller beslut om sanktionsavgift mot myndigheter får antas att dessa blir sällsynta. Det beror dels på att myndigheter i regel kan förväntas anpassa verksamheten efter Datainspektionens synpunkter utan att det krävs repressiva åtgärder, dels på att sanktionsavgift är den åtgärd som tillsynsmyndigheten bör välja i sista hand. Det bör därför inte påverka Datainspektionens arbetsbörda i någon större utsträckning. Eftersom sanktionsavgifterna kan vara kännbara ekonomiskt är det rimligt att utgå från att inspektionens beslut kommer att överklagas till allmän förvaltningsdomstol i relativt stor utsträckning. Det faktum att sådana beslut förväntas bli ovanliga innebär dock att även överklagandena bör bli sällsynta.

Kostnaderna för Datainspektionen och de allmänna förvaltningsdomstolarna bör därför rymmas inom befintliga anslagsramar såvitt avser förslagen i detta betänkande. De förändringar dataskyddsförordningen i övrigt medför kommer sannolikt att kräva budgetförstärkningar, framför allt för Datainspektionen. Detta ligger emellertid utanför vårt uppdrag att bedöma.

21.3.2 Ekonomiska konsekvenser för enskilda

Utredningens bedömning: Förslagen medför inga nya kostnader eller någon ökad administrativ börda för enskilda.

De konsekvenser som beskrivs här avser som nämnts tidigare enbart våra förslag och inte dataskyddsförordningens bestämmelser i stort. Vår analys utgår vidare från de förändringar som våra förslag medför i relation till vad som gäller enligt nuvarande generella reglering, dvs. personuppgiftslagen och personuppgiftsförordningen. Med dessa utgångspunkter bedöms förslagen i detta betänkande inte leda till några kostnadsökningar eller någon ökad administrativ börda för enskilda.

21.4 Konsekvenser i övrigt

Utredningens bedömning: Förslagen förväntas förbättra skyddet för enskildas personliga integritet och minskar antalet kriminaliserade handlingar. De förväntas inte få några andra konsekvenser.

Enskildas personliga integritet

Förslagen innebär bland annat att det införs särskilda undantag för myndigheternas behandling av känsliga personuppgifter. Avsikten med förslagen i denna del är inte att utvidga möjligheterna till behandling i relation till vad som gäller i dag, utan att i stort sett möjliggöra behandling i motsvarande utsträckning som enligt personuppgiftslagen och personuppgiftsförordningen. Vi föreslår dock också ett förbud för myndigheter som behandlar uppgifter med stöd av nämnda undantag att använda sökbegrepp som avslöjar känsliga personuppgifter. Sökförbudet saknar motsvarighet i dag. Vi bedömer att det förslaget gynnar enskildas personliga integritet.

Dataskyddsförordningens bestämmelser innebär en förstärkning av enskildas rätt till information och tillgång till personuppgifter jämfört med motsvarande reglering i personuppgiftslagen. De undantag vi föreslår från förordningens bestämmelser i detta avseende motsvarar de befintliga undantagen i personuppgiftslagen, trots att mer långtgående undantag i och för sig hade varit möjliga. Vi bedömer därför att regleringen sammantaget innebär en förstärkning av skyddet för enskildas personliga integritet.

Vidare ger förslagen enskilda ökade möjligheter att reagera om deras klagomål hos tillsynsmyndigheten inte behandlas i tid, och att föra en dröjsmålstalan mot tillsynsmyndigheten i vissa fall. Detta bedöms också öka skyddet för enskildas personliga integritet, liksom den föreslagna möjligheten att besluta om sanktionsavgifter mot myndigheter när det gäller felaktig behandling av enskildas personuppgifter. Den föreslagna tystnadsplikten för dataskyddsombud innebär slutligen också ett stärkt skydd för den personliga integriteten.

Övrigt

Förslagen kommer att gälla även för personuppgiftsbehandling som sker hos kommuner och landsting men får inte några särskilda konsekvenser för dessa organ eller för den kommunala självstyrelsen.

Eftersom vi inte föreslår att någon straffbestämmelse motsvarande den som finns i personuppgiftslagen ska införas i dataskyddslagen minskar förslagen antalet kriminaliserade handlingar. I övrigt har förslagen inte några konsekvenser för brottsligheten eller det brottsförebyggande arbetet.

Författningsförslagen är könsneutralt utformade och förväntas inte få några konsekvenser för jämställdheten mellan kvinnor och män.

Förslagen får inte några andra sådana konsekvenser som avses i 14–15 a §§ kommittéförordningen.

22 Författningskommentar

22.1 Förslaget till lag med kompletterande bestämmelser till EU:s dataskyddsförordning

1 kap. Inledande bestämmelser

1 § Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), nedan kallad dataskyddsförordningen.

Termer och uttryck som används i denna lag har samma betydelse som i dataskyddsförordningen.

Paragrafen anger lagens innehåll. Hänvisningarna till dataskyddsförordningen i denna lag är med undantag för 2 § dynamiska, dvs. avser förordningen i dess vid varje tidpunkt gällande lydelse. Övervägandena finns i avsnitt 5.2.2.

I första stycket anges att lagen innehåller kompletterande bestämmelser till EU:s dataskyddsförordning. Dataskyddsförordningen är direkt tillämplig i varje medlemsstat. Det innebär att den automatiskt är en del av den svenska rättsordningen. I vissa avseenden förutsätter eller tillåter dataskyddsförordningen emellertid att Sverige inför bestämmelser som kompletterar förordningen, antingen i form av preciseringar eller i form av undantag. Denna lag innehåller de kompletterande bestämmelser som gäller på ett generellt plan. Vid sidan av denna lag finns det även sektorsspecifika författningar som innehåller bestämmelser som kompletterar dataskyddsförordningen på avgränsade områden.

Av *andra stycket* framgår att de termer och uttryck som används i lagen ska förstås på samma sätt som i dataskyddsförordningen. Det innebär bland annat att definitionerna i artikel 4 i dataskyddsförordningen även gäller vid tillämpningen av lagen.

2 § Bestämmelserna i dataskyddsförordningen, i den ursprungliga lydelsen, och i denna lag ska i tillämpliga delar gälla även vid behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten och i verksamhet som omfattas av avdelning V kapitel 2 i fördraget om Europeiska unionen.

Paragrafen avser det materiella tillämpningsområdet för dataskyddsförordningens bestämmelser och har ingen motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 6.4.

Bestämmelsen innebär att förordningens bestämmelser gäller som svensk rätt vid personuppgiftsbehandling som utförs i sådan verksamhet som enligt artikel 2.2 a och 2.2 b i dataskyddsförordningen är undantagen från förordningens tillämpningsområde. Förordningens bestämmelser gäller alltså, i tillämpliga delar, även vid personuppgiftsbehandling som utförs som ett led i en verksamhet som inte omfattas av unionsrätten och i verksamhet som utförs inom ramen för den gemensamma utrikes- och säkerhetspolitiken. Verksamhet som inte omfattas av unionsrättens tillämpningsområde är bland annat verksamhet som rör nationell säkerhet och verksamhet på försvarsområdet.

Det är inte möjligt att genom nationell rätt ålägga tillsynsmyndigheter i andra länder att samarbeta med den svenska tillsynsmyndigheten. De bestämmelser i förordningen som avser tillsynsmyndigheternas skyldighet att samarbeta med varandra är därför inte tillämpliga. Inte heller är det möjligt att genom nationell rätt ge den europeiska dataskyddsstyrelsen behörighet att t.ex. utfärda riktlinjer och rekommendationer eller att ge kommissionen rätt att anta delegerade akter inom detta område. Kapitel VII och kapitel X i dataskyddsförordningen utgör därför inte "tillämpliga delar". Det kan även i övrigt finnas bestämmelser i dataskyddsförordningen som inte kan tillämpas i rent nationell verksamhet. Det får därför i varje enskilt fall göras en bedömning av om en viss förordningsbestämmelse kan gälla.

Det bör noteras att det i sektorsspecifika författningar som avser verksamhet utanför dataskyddsförordningens egentliga tillämpnings-

område kan föreskrivas undantag från bestämmelsen, se 3 §. Det kan i sådana författningar även anges att endast vissa av förordningens bestämmelser inte ska gälla inom just det området.

Hänvisningen till dataskyddsförordningen i denna paragraf är statisk, dvs. avser den ursprungliga lydelsen av förordningen.

3 § Om en annan lag eller en förordning innehåller någon bestämmelse som rör behandling av personuppgifter och som avviker från denna lag tillämpas den bestämmelsen.

Paragrafen avser lagens förhållande till avvikande bestämmelser i andra författningar. Bestämmelsen motsvarar i sak 2 § PUL. Övervägandena finns i avsnitt 5.2.3.

Bestämmelsen innebär att avvikande bestämmelser som rör behandling av personuppgifter och som finns i en annan lag eller i en förordning ska ha företräde framför lagen. Det kan t.ex. vara bestämmelser som specificerar den rättsliga grunden för en myndighets behandling av personuppgifter, begränsningar av rätten att behandla känsliga personuppgifter i en viss verksamhet eller särskilda förfaranderegler. Sådana avvikande bestämmelser som avses i paragrafen finns ofta i författningar som helt eller delvis innehåller bestämmelser om behandling av personuppgifter hos en viss myndighet, inom en viss sektor eller i ett visst sammanhang. Sådana författningar förekommer främst inom den offentliga sektorn.

Beslut som riksdagen eller regeringen har fattat i annan form än lag eller förordning och föreskrifter som myndigheter har utfärdat tar däremot inte över bestämmelserna i denna lag. Bestämmelsen innebär inte heller att avvikande bestämmelser per automatik har företräde framför dataskyddsförordningen. Sådant företräde gäller endast i den mån förordningen tillåter nationell särreglering.

Formuleringen ”i en annan lag” omfattar inte bara avvikande bestämmelser i lagar antagna av den svenska riksdagen, utan även bestämmelser i direkt tillämpliga EU-förordningar.

Frågan om en viss bestämmelse innefattar en avvikelse från vad som ska gälla enligt denna lag får avgöras med tillämpning av sedvanliga metoder för tolkning av författningar. Eventuella normkonflikter mellan bestämmelserna i denna lag och bestämmelser i annan författning om annat än dataskydd får på motsvarande sätt lösas med hjälp av allmänna principer, som till exempel att grundlag har före-

träde framför vanlig lag, att EU-rätten har företräde framför svensk lag och att speciallag har företräde framför generell lag.

4 § Bestämmelserna i dataskyddsförordningen och i denna lag ska inte tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Bestämmelserna i kapitel II och III, artiklarna 24–30 och 35–43 och kapitel V i dataskyddsförordningen samt i 2–5 kap. denna lag ska inte tillämpas på behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

Paragrafen avser dataskyddsförordningens och lagens förhållande till tryck- och yttrandefriheten och motsvarar 7 § PUL. Övervägandena finns i avsnitt 7.4.

Bestämmelsen i *första stycket* erinrar om att tryckfrihetsförordningen och yttrandefrihetsgrundlagens bestämmelser om tryck- och yttrandefrihet har företräde framför dataskyddsförordningens och lagens bestämmelser. Att bestämmelserna om allmänhetens tillgång till handlingar i tryckfrihetsförordningens 2 kap. har företräde framför dataskyddsförordningens bestämmelser följer av artikel 86 i förordningen.

I *andra stycket* undantas uppräknade kapitel och artiklar i dataskyddsförordningen och i lagen när det gäller behandling för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande *utanför* det grundlagsreglerade området. Bestämmelsen har sin grund i artikel 85.2 i dataskyddsförordningen och innebär i sak att bestämmelserna om syfte, tillämpningsområde och definitioner (kapitel I), om samarbete med tillsynsmyndigheten och säkerhet för personuppgifter (artiklarna 31–34 i kapitel IV), om oberoende tillsynsmyndigheter (kapitel VI), om samarbete och enhetlighet (kapitel VII) samt om rättsmedel, ansvar och sanktioner (kapitel VIII) är tillämpliga på behandling för de nämnda ändamålen. Det bör noteras att bestämmelserna om tillsyn, rättsmedel, ansvar och sanktioner alltså enbart blir tillämpliga såvitt avser tillsyn över eller överträdelser av bestämmelserna om säkerhet för personuppgifter. Kapitel IX, X och XI är i och för sig inte undantagna men bedöms i praktiken inte

aktualiseras vid behandling för sådana ändamål som avses i paragrafen.

5 § Vid tillämpningen av 3 kap. 3 § 2 och 4 § samt 4 kap. 1 § andra stycket ska andra organ än myndigheter jämföras med myndigheter, i den utsträckning bestämmelserna om allmänna handlingar och sekretess i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400) gäller i organets verksamhet.

Paragrafen avser organ som ska jämföras med myndigheter. Bestämmelsen saknar motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 10.6.2 och 14.4.6.

Bestämmelsen innebär att vissa bestämmelser i lagen ska gälla även för andra organ än myndigheter, i den mån offentlighetsprincipen och sekretesslagstiftningen enligt författning gäller i organets verksamhet. Bestämmelsens hänvisning till 3 kap. 3 § 2 möjliggör sådan behandling av känsliga personuppgifter som är oundviklig i organets verksamhet som en direkt följd av bland annat tryckfrihetsförordningens och offentlighets- och sekretesslagens bestämmelser om allmänna handlingar och diarieföring. Sökförbudet i 3 kap. 4 § avseende känsliga personuppgifter ska gälla vid sådan tillämpning. Bestämmelsens hänvisning till 4 kap. 1 § andra stycket innebär att användningsbegränsningen i första stycket samma paragraf inte hindrar organ som omfattas av offentlighetsprincipen från att använda personuppgifter som finns i allmänna handlingar.

6 § Den som utsetts till dataskyddsbud enligt artikel 37 i dataskyddsförordningen får inte obehörigen röja det som han eller hon vid fullgörandet av sin uppgift har fått veta om enskilds personliga och ekonomiska förhållanden.

I det allmännas verksamhet tillämpas offentlighets- och sekretesslagen (2009:400) i stället för första stycket.

Paragrafen innebär att tystnadsplikt gäller för dataskyddsbud, och saknar motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 17.4.3.

Bestämmelsen har stöd i dataskyddsförordningens artikel 38.5. Tystnadsplikten i första stycket är begränsad till obehörigt röjande av uppgifter. Begränsningen innebär att uppgifter exempelvis får lämnas

ut med samtycke, till tillsynsmyndighet eller annars som en följd av en skyldighet i lag eller annan författning.

Andra stycket innehåller en erinran om att offentlighets- och sekretesslagen tillämpas i det allmännas verksamhet. Så länge dataskyddsombudet innehar en sådan anställning eller uppdrag som avses i 2 kap. 1 § andra stycket OSL omfattas han eller hon av sekretessen. Ett dataskyddsombud får i allmänhet anses delta i verksamheten på ett sådant sätt som förutsätts i nämnda paragraf. Om ett dataskyddsombud inte omfattas av bestämmelserna i offentlighets- och sekretesslagen gäller tystnadspliktsbestämmelsen i första stycket för uppgifter som han eller hon fått kännedom om inom ramen för sitt uppdrag.

2 kap. Rättslig grund

1 § Av dataskyddsförordningen framgår att personuppgifter får behandlas endast om minst ett av de villkor som anges i artikel 6.1 i förordningen är uppfyllt.

Paragrafen upplyser om att motsvarigheten till 10 § PUL, som anger villkoren för laglig behandling, finns i artikel 6.1 i dataskyddsförordningen. Övervägandena finns i avsnitt 8.3.6.

Uppräkningen i artikel 6.1 i dataskyddsförordningen är uttömmande. Om ingen av dessa punkter är tillämpliga är behandlingen inte laglig och får därmed inte utföras. De olika punkterna är i viss mån överlappande. Flera punkter kan därför vara tillämpliga avseende en och samma behandling.

Den omständigheten att behandlingen är laglig enligt artikel 6.1 i dataskyddsförordningen, dvs. att det finns en tillämplig rättslig grund, innebär inte att behandling kan ske av vilka uppgifter som helst eller på valfritt sätt. Den personuppgiftsansvarige måste också uppfylla kraven i övriga bestämmelser i förordningen och i bestämmelser som kompletterar förordningen.

För att en behandling av personuppgifter ska vara tillåten enligt artikel 6.1 b–f måste den vara nödvändig för att fullgöra, skydda eller utföra den rättsliga grunden. Detta innebär inte ett krav på att behandlingsåtgärden ska vara oundgänglig, att den inte kan underlåtas. Behandlingen kan under vissa omständigheter anses vara nöd-

vändig och därmed tillåten enligt artikel 6, om behandlingen leder till effektivitetsvinster.

2 § Vid erbjudande av informationssamhällets tjänster direkt till ett barn, ska vid tillämpningen av artikel 6.1 a i dataskyddsförordningen behandling av personuppgifter som rör ett barn vara tillåten om barnet är minst 13 år. Om barnet är under 13 år ska sådan behandling vara tillåten endast om och i den mån samtycke ges eller godkänns av den person som har föräldraansvar för barnet.

Paragrafen anger vid vilken ålder barn som erbjuds informations-samhällets tjänster själva kan samtycka till behandling av personuppgifter. Paragrafen har ingen motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 9.5.

Bestämmelsen har sin grund i artikel 8.1 i dataskyddsförordningen, som anger att sådan behandling av personuppgifter som avses i paragrafen får ske med stöd av barnets eget samtycke om barnet har fyllt 16 år. Medlemsstaterna får föreskriva en lägre åldersgräns, dock lägst 13 år.

Informationssamhällets tjänster är tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare. Det rör sig således om t.ex. sociala medier, söktjänster och s.k. appar på smarta enheter. Bestämmelsen är tillämplig endast när den rättsliga grunden för personuppgifts-behandlingen är samtycke och inte när behandlingen utförs på annan rättslig grund. Om barnet är under 13 år får behandling av personuppgifter med stöd av samtycke ske endast om samtycket ges eller godkänns av den person som har föräldraansvar för barnet. Denna person är i allmänhet barnets vårdnadshavare. Om barnet inte har en vårdnadshavare eller vårdnadshavarna inte kan eller får utöva vårdnaden, får det från fall till fall bedömas vem som kan samtycka till personuppgiftsbehandlingen rörande barnet eller godkänna barnets samtycke.

3 § Personuppgifter får behandlas med stöd av artikel 6.1 c i dataskyddsförordningen om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som

- 1. gäller enligt lag eller annan författning,*
- 2. följer av kollektivavtal, eller*

3. följer av beslut som har meddelats med stöd av lag eller annan författning.

Paragrafen upplyser om att en rättslig förpliktelse utgör en rättslig grund för behandling av personuppgifter endast om förpliktelsen är fastställd i enlighet med unionsrätten eller den nationella rätten. Kravet på fastställande saknar motsvarighet i personuppgiftslagen. Att en rättslig förpliktelse kan utgöra rättslig grund för personuppgiftsbehandling enligt personuppgiftslagen framgår av 10 § b PUL. Övervägandena finns i avsnitt 8.3.1 och 8.3.2.

Bestämmelsen har sin grund i artikel 6.3 första stycket i dataskyddsförordningen. För att en förpliktelse som åligger den personuppgiftsansvarige ska kunna läggas till grund för behandling av personuppgifter måste den vara rättsligt förankrad och giltig. En förpliktelse som inte är rättsligt förankrad i unionsrätten eller i medlemsstatens nationella rätt kan inte återopas som rättslig grund för behandling av personuppgifter. Förpliktelsen måste alltså ha meddelats i laga ordning, men behöver inte för den skull framgå direkt av en författning. Enligt svensk rätt kan en rättslig förpliktelse även framgå av t.ex. kollektivavtal, regeringsbeslut och myndighetsbeslut. Formuleringarna ”gäller enligt lag” och ”med stöd av lag” omfattar även förpliktelser som följer av direkt tillämpliga unionsrättsakter, eftersom unionsrättsakter gäller här i landet med den verkan som följer av EU-fördragen.

Det bör noteras att bestämmelsen i artikel 6.3 andra stycket första meningen i dataskyddsförordningen anger att syftet med behandlingen ska fastställas i den rättsliga grunden. Kravet torde innebära att en förpliktelse inte kan läggas till grund för behandling av personuppgifter om syftet med behandlingen inte framgår av den författning eller det kollektivavtal som förpliktelsen grundas på och inte heller, i förekommande fall, kan utläsas av det beslut som anger förpliktelsen.

4 § Personuppgifter får behandlas med stöd av artikel 6.1 e i dataskyddsförordningen om behandlingen är nödvändig

1. för att den personuppgiftsansvarige ska kunna utföra en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning, eller

2. som ett led i den personuppgiftsansvariges myndighetsutövning enligt lag eller annan författning.

Paragrafen upplyser om att en uppgift av allmänt intresse liksom myndighetsutövning utgör rättslig grund för behandling av personuppgifter endast om uppgiften eller myndighetsutövningen är fastställd i enlighet med unionsrätten eller den nationella rätten. Kravet på fastställande saknar motsvarighet i personuppgiftslagen. Att en uppgift av allmänt intresse och myndighetsutövning kan utgöra rättslig grund för personuppgiftsbehandling framgår dock av 10 § d respektive e PUL. Övervägandena finns i avsnitt 8.3.1, 8.3.3 och 8.3.4.

Bestämmelsen, som har sin grund i artikel 6.3 första stycket i dataskyddsförordningen, förtydligar att en uppgift av allmänt intresse respektive myndighetsutövning som inte är rättsligt förankrad i unionsrätten eller i medlemsstatens nationella rätt inte kan åberopas som rättslig grund för behandling av personuppgifter. I artikel 6.3 andra stycket i dataskyddsförordningen anges att syftet med behandlingen måste vara nödvändigt för att utföra uppgiften eller myndighetsutövningen. Den specifika behandlingen måste alltså vara nödvändig för ett ändamål som i sin tur är nödvändigt för att den personuppgiftsansvarige ska kunna utföra sin fastställda uppgift.

I *punkt 1* tydliggörs att en uppgift av allmänt intresse utgör en rättslig grund för behandling av personuppgifter bara om uppgiften följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Denna förutsättning gäller oavsett om den personuppgiftsansvarige är en myndighet eller inte. Det är alltså inte tillräckligt att uppgiften är av allmänt intresse – uppgiften måste också vara fastställd i enlighet med gällande rätt.

Statliga och kommunala myndigheters verksamhet är i allt väsentligt av allmänt intresse. Formuleringen, ”som följer av lag eller annan författning”, är en följd av att en uppgift av allmänt intresse enligt svensk rätt inte måste vara uttryckt i lag eller förordning utan också kan anges i en annan föreskrift, förutsatt att föreskriften har meddelats med stöd av lag eller förordning. Som en följd av den svenska arbetsmarknadsmodellen skulle en uppgift av allmänt intresse även kunna vara fastställd genom kollektivavtal. Uppgifter av allmänt intresse kan enligt svensk rätt även fastställas genom ”beslut som meddelats med stöd av lag eller annan författning”. Till exempel kan

en sådan uppgift ha tilldelats en statlig myndighet eller ett statligt bolag med särskilt samhällsintresse genom regeringsbeslut. Formuleringen omfattar även uppgifter som med stöd av kommunallagen har getts till kommunala myndigheter och kommunala bolag genom beslut i fullmäktige. EU-rättsakter gäller här i landet med den verkan som följer av fördragen, vilket innebär att uppgifter som utförs enligt unionsrätten även utförs enligt lag. Den föreslagna formuleringen omfattar således även sådana uppgifter.

Även privaträttsligt bedriven verksamhet av allmänt intresse omfattas av formuleringen, förutsatt att verksamheten är reglerad i lag eller annan författning eller följer av kollektivavtal eller av beslut som meddelats med stöd av lag eller annan författning. Däremot omfattas inte oreglerad verksamhet. Formuleringen omfattar inte heller sådan verksamhet som i och för sig är reglerad, men som inte kan anses vara av allmänt intresse i unionsrättslig mening.

Det bör noteras att den författning eller det kollektivavtal eller beslut som utgör den rättsliga grunden för behandling av personuppgifter måste uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas (artikel 6.3 andra stycket sista meningen i dataskyddsförordningen).

I *punkt 2* tydliggörs på motsvarande sätt att myndighetsutövning utgör en rättslig grund för behandling av personuppgifter bara om myndighetsutövningen sker enligt lag eller annan författning. Detta gäller oavsett om den personuppgiftsansvarige är en myndighet eller inte. Om författningen ställer ytterligare villkor, t.ex. krav på att ett privat organ ska vara certifierat för att få utöva myndighet, sker myndighetsutövningen "enligt" författningen om villkoret är uppfyllt. Formuleringen "enligt lag eller annan författning" innefattar t.ex. förordningar som har meddelats av regeringen, med stöd av restkompetensen. Formuleringen innefattar även befogenheter som anges i myndighetsföreskrifter, förutsatt att föreskrifterna har meddelats med stöd av ett bemyndigande. Unionsrättsakter gäller här i landet med den verkan som följer av EU-fördragen, vilket innebär att myndighetsutövning som utövas enligt unionsrätten också har stöd av lag. Formuleringen omfattar således även sådana befogenheter.

5 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om behandling av personuppgifter för arkivändamål av allmänt intresse, när det gäller andra enskilda organ än de som

omfattas av bestämmelserna om allmänna handlingar och sekretess i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400).

Den myndighet som regeringen bestämmer får även i enskilda fall besluta att sådana enskilda organ som avses i första stycket får behandla personuppgifter för arkivändamål av allmänt intresse.

Paragrafen innehåller ett bemyndigande avseende föreskrifter och förvaltningsbeslut om behandling av personuppgifter för arkivändamål av allmänt intresse utanför arkivlagstiftningens tillämpningsområde. Bestämmelsen saknar motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 14.4.2.

Bestämmelserna har sin grund i artikel 6.3 första stycket i dataskyddsförordningen, som innebär att en uppgift av allmänt intresse utgör rättslig grund för behandling av personuppgifter endast om uppgiften är fastställd i enlighet med unionsrätten eller den nationella rätten. Bestämmelserna gör det möjligt för enskilda arkivinstitutioner, vars uppgift inte redan är fastställd i enlighet med gällande rätt, att få sin verksamhet prövad och godkänd som rättslig grund för personuppgiftsbehandling.

Rättslig grund kan antingen fastställas i föreskrifter som meddelas enligt *första stycket*, eller i förvaltningsbeslut som meddelas enligt *andra stycket*. En förutsättning i båda fallen är att arkivverksamheten är av allmänt intresse i dataskyddsförordningens mening och att organet inte är en myndighet eller ett sådant organ som enligt 1 kap. 5 § ska jämföras med myndigheter. Den rättsliga grunden för behandling av personuppgifter i myndigheters och därmed jämförda organs arkivverksamhet är redan fastställd i arkivlagstiftningen.

3 kap. Vissa kategorier av personuppgifter

1 § Utöver vad som framgår av artikel 9.2 a, c, d, e eller f i dataskyddsförordningen får sådana särskilda kategorier av personuppgifter som anges i artikel 9.1 i dataskyddsförordningen (känsliga personuppgifter) behandlas om förutsättningarna i någon av 2–8 §§ är uppfyllda.

Paragrafen anger lagens förhållande till undantagen från förbudet att behandla känsliga personuppgifter i förordningens artikel 9.2. För-

budet mot behandling av känsliga personuppgifter och undantagen från det förbudet har sin motsvarighet i 13–19 §§ PUL. Övervägandena finns i avsnitt 10.3.

Bestämmelsen förtydligar att vissa av förordningens undantag från förbudet är direkt tillämpliga, dvs. artikel 9.2 a (samtycke), 9.2 c (den registrerades eller annans grundläggande intressen), 9.2 d (ideella organisationer), 9.2 e (offentliggörande) och 9.2 f (rättsliga anspråk och dömande verksamhet).

Utöver de direkt tillämpliga undantagen får behandling av känsliga personuppgifter ske med stöd av 2–8 §§ i lagen, vilka i sin tur har införts i svensk rätt med stöd av förordningens undantag i artikel 9.2 b, g, h och j. Observera dock att undantag som tillåter behandling i andra fall kan finnas i sektorsspecifik reglering.

2 § Känsliga personuppgifter får med stöd av artikel 9.2 b i dataskyddsförordningen behandlas om det är nödvändigt för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten.

Personuppgifter som behandlas med stöd av första stycket får lämnas ut till tredje part endast om det inom arbetsrätten finns en skyldighet att göra det eller om den registrerade uttryckligen har samtyckt till utlämnandet.

Paragrafen anger när känsliga personuppgifter får behandlas på arbetsrättens område. Paragrafen har sin motsvarighet i 16 § första stycket a PUL samt andra stycket samma paragraf. Övervägandena finns i avsnitt 10.5.2.

Bestämmelsen i *första stycket* har sin grund i artikel 9.2 b i dataskyddsförordningen. Termen ”inom arbetsrätten” är ett unionsrättsligt begrepp som måste tolkas EU-konformt. I avsaknad av andra tolkningsdata bör begreppet även fortsättningsvis ges den tolkning som den har enligt personuppgiftslagen. I stort sett alla skyldigheter och rättigheter för arbetsgivare beträffande de anställda och deras organisationer bör alltså kunna innefattas i uttrycket inom arbetsrätten, exempelvis behandling i samband med sjuklön och rehabilitering av arbetstagare. Även skyldigheter och rättigheter för fackliga organisationer i förhållande till arbetsgivare och deras organisationer bör innefattas. Att undantaget i artikel 9.2 b gäller även behandling

som sker enligt kollektivavtal framgår av artikeltexten, vilken också innebär att lämpliga skyddsåtgärder måste framgå av avtalet.

I *andra stycket* begränsas möjligheterna att lämna ut uppgifter som behandlas med stöd av första stycket. Den skyldighet att lämna ut uppgifter som avses är sådan som åligger den personuppgiftsansvarige enligt författning, myndighetsbeslut eller avtal på arbetsrättens område. Termen tredje part definieras i förordningens artikel 4.10 som en fysisk eller juridisk person, offentlig myndighet, institution eller ett organ som inte är den registrerade, den personuppgiftsansvarige, personuppgiftsbiträdet eller de personer som under den personuppgiftsansvariges eller personuppgiftsbitrådets direkta ansvar är behöriga att behandla personuppgifterna. Detta innebär exempelvis att en arbetsgivares utlämnande till en facklig organisation omfattas av regleringen.

Andra stycket innebär ingen begränsning av allmänhetens rätt till tillgång till handlingar. Det följer av förordningens artikel 86 att allmänhetens rätt till tillgång till handlingar enligt tryckfrihetsförordningen gäller före förordningens bestämmelser om personuppgiftsskydd.

3 § Känsliga personuppgifter får med stöd av artikel 9.2 g i dataskyddsförordningen behandlas av en myndighet

1. i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av ett ärende,

2. om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag, eller

3. i enstaka fall, om det är absolut nödvändigt för ändamålet med behandlingen och behandlingen inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

Paragrafen innebär att myndigheter får behandla känsliga personuppgifter i vissa fall. Bestämmelsen i första punkten motsvarar 8 § PUF. Övervägandena finns i avsnitt 10.6.2.

Bestämmelserna har sin grund i artikel 9.2 g i dataskyddsförordningen om behandling som är nödvändig av hänsyn till ett viktigt allmänt intresse.

Punkt 1 möjliggör behandling av känsliga personuppgifter i myndigheternas ärenden, förutsatt att uppgifterna förekommer i löpande text och inte har strukturerats i registerform eller på annat sätt

sorterats. Bestämmelsen utesluter dock inte att handlingar som innehåller löpande text med ostrukturerade känsliga personuppgifter lagras elektroniskt i ärendehanteringssystem eller liknande. Uppgifterna måste ha lämnats in av någon utomstående eller vara nödvändiga för handläggningen av ärendet.

Punkt 2 möjliggör sådan behandling av känsliga personuppgifter som är oundviklig i myndigheternas verksamhet som en direkt följd av framför allt tryckfrihetsförordningens, offentlighets- och sekretesslagens och förvaltningslagens bestämmelser om hur inkomna handlingar ska hanteras, exempelvis genom krav på diarieföring och skyldighet att ta emot e-post. Behandling av känsliga personuppgifter med stöd av denna punkt får bara ske om uppgifterna har lämnats in till myndigheten, dvs. uppgifter i handlingar som definieras som inkomna enligt 2 kap. 6 § tryckfrihetsförordningen, och själva behandlingen av uppgifterna är ett direkt krav enligt annan lag. Det bör noteras att enligt 1 kap. 5 § ska bestämmelsen i denna punkt gälla även för andra organ än myndigheter, i den mån offentlighetsprincipen och sekretesslagstiftningen enligt författning gäller i organets verksamhet.

Punkt 3 möjliggör behandling av känsliga personuppgifter hos myndigheter i enstaka fall även då behandlingen inte sker i löpande text med koppling till visst ärende eller krävs enligt annan lag. Så kan exempelvis vara fallet i faktisk verksamhet såsom i kommunikation mellan skola och föräldrar eller inom en myndighet i samband med utvärdering.

Kravet i punkt 3 på att behandlingen ska vara absolut nödvändig för ändamålet med behandlingen innebär att undantaget ska tillämpas restriktivt och att behovet av att behandla den känsliga personuppgiften i det enskilda fallet noga ska prövas mot ändamålet med behandlingen.

Vidare ställer bestämmelsen i punkt 3 krav på att ytterligare en avvägning ska göras för att behandling av känsliga personuppgifter ska få ske i det enskilda fallet. Det krävs en prövning av om en i och för sig absolut nödvändig behandling av känsliga personuppgifter ändå innebär ett otillbörligt intrång i den registrerades integritet. Vid bedömningen av om behandling utgör ett otillbörligt intrång ska vikt läggas vid sådana aspekter som uppgifternas känslighet, den inställning de registrerade kan antas ha till att uppgiften behandlas, den spridning uppgiften skulle komma att få och risken för vidarebehandling för andra ändamål än insamlingsändamålet.

4 § Vid behandling som sker enbart med stöd av 3 § får en myndighet inte använda sökbegrepp som avslöjar känsliga personuppgifter.

Paragrafen innebär att det gäller ett förbud för myndigheter att söka på känsliga personuppgifter då sådana uppgifter behandlas enbart med stöd av 3 §. Sådana sökningar kan dock tillåtas i sektorsspecifik reglering. Paragrafen har ingen motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 10.6.2.

Sökförbudet införs för att tillgodose kraven på särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen i artikel 9.2 g i dataskyddsförordningen. Förbudet omfattar alla tekniska åtgärder, som innebär att uppgifter används för att strukturera eller systematisera information så att känsliga personuppgifter avslöjas.

Sökförbudet innebär att offentlighetsprincipen inskränks enligt den så kallade begränsningsregeln i 2 kap. 3 § tredje stycket tryckfrihetsförordningen. En begäran att få tillgång till en sammanställning av uppgifter som är resultatet av en sådan förbjuden sökning ska alltså avslås på den grunden att sammanställningen inte anses förvarad hos myndigheten. Det bör dock understrykas att begränsningsregeln inte hindrar att sökningar görs i färdiga elektroniska handlingar vid en begäran om tillgång till allmänna handlingar, dvs. sökning får på begäran ske i upptagningar där myndigheten eller den som lämnat in handlingen till myndigheten har gett upptagningen ett bestämt, fixerat, innehåll som går att återskapa gång på gång.

Det bör noteras att enligt 1 kap. 5 § ska sökförbudet gälla även för andra organ än myndigheter, som på grund av att offentlighetsprincipen och sekretesslagstiftningen enligt författning gäller i organets verksamhet behandlar känsliga personuppgifter med stöd av 3 § 2.

5 § Känsliga personuppgifter får med stöd av artikel 9.2 h i dataskyddsförordningen behandlas om behandlingen är nödvändig av skäl som hör samman med

- 1. förebyggande hälso- och sjukvård och yrkesmedicin,*
- 2. bedömningen av en arbetstagares arbetskapacitet,*
- 3. medicinska diagnoser,*
- 4. tillhandahållande av hälso- och sjukvård eller behandling,*
- 5. social omsorg, eller*

6. förvaltning av social omsorg, hälso- och sjukvårdstjänster samt deras system.

Behandling enligt första stycket får ske under förutsättning att kravet på tystnadsplikt i artikel 9.3 i dataskyddsförordningen är uppfyllt.

Paragrafen anger när känsliga personuppgifter inom social omsorg samt på hälso- och sjukvårdsområdet får behandlas när någon sektorsspecifik reglering som tillåter sådan behandling inte finns. Bestämmelserna motsvarar delvis 18 § PUL. Övervägandena finns i avsnitt 10.7.2.

Paragrafen har sin grund i artikel 9.2 h i dataskyddsförordningen. I första stycket punkterna 1–6 anges de ändamål för vilka behandling av känsliga personuppgifter får ske. Begreppen motsvarar de som anges i artikel 9.2 h och måste ges en EU-rättslig innebörd.

Andra stycket erinrar om kravet på tystnadsplikt i förordningens artikel 9.3. Sammantaget innebär paragrafens första stycke och artikel 9.3 att behandling av känsliga personuppgifter bara är tillåten för de i paragrafen angivna ändamålen, och enbart under förutsättning att behandlingen sker av eller under ansvar av en person som omfattas av tystnadsplikt enligt unionsrätten eller svensk rätt.

6 § *Känsliga personuppgifter får med stöd av artikel 9.2 j i dataskyddsförordningen behandlas för arkivändamål av allmänt intresse om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om bevarande och vård av arkiv.*

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att känsliga personuppgifter får behandlas för arkivändamål av allmänt intresse även i andra fall än de som avses i första stycket.

Den myndighet som regeringen bestämmer får även i enskilda fall besluta att andra enskilda organ än de som omfattas av bestämmelserna om allmänna handlingar och sekretess i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400) får behandla känsliga personuppgifter för arkivändamål av allmänt intresse.

Paragrafen avser behandling av känsliga personuppgifter för arkivändamål av allmänt intresse och motsvarar delvis 8 § andra stycket första meningen PUL. Övervägandena finns i avsnitt 14.4.3.

Bestämmelsen, som har sin grund i artikel 9.2 j i dataskyddsförordningen, avser undantag från förordningens förbud mot att behandla känsliga personuppgifter, vid behandling av personuppgifter för arkivändamål av allmänt intresse. Möjligheten att för sådana ändamål behandla personuppgifter om lagöverträdelser regleras i 9 och 11 §§. Behandling av andra slags uppgifter för arkivändamål av allmänt intresse regleras i stället av direkt tillämpliga bestämmelser i förordningen. Det följer också direkt av förordningen att vidarebehandling av personuppgifter för arkivändamål av allmänt intresse inte ska anses som oförenlig med de ursprungliga ändamålen. Det behövs inte heller någon separat rättslig grund för en sådan vidarebehandling.

För att känsliga personuppgifter ska få behandlas för arkivändamål av allmänt intresse enligt *första stycket* krävs att behandlingen sker som en följd av de skyldigheter att bevara och vårda handlingar som anges i föreskrifter. Detta krav gäller oavsett om personuppgifterna samlas in för arkivändamål av allmänt intresse eller om uppgifter som samlats in för andra ändamål vidarebehandlas för arkivändamål av allmänt intresse. På generell nivå anges sådana skyldigheter i arkivlagen och arkivförordningen samt i Riksarkivets och andra arkivmyndigheters föreskrifter. Det utrymme för behandling av känsliga personuppgifter för arkivändamål av allmänt intresse som första stycket ger är därmed i första hand tillgängligt för myndigheter och andra organ som omfattas av arkivlagstiftningen. Bestämmelsen medför, tillsammans med 11 §, att dataskyddsförordningen och lagen inte hindrar att en myndighet eller ett annat organ som omfattas av offentlighetsprincipen arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet.

I *andra stycket* bemyndigas regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter som tillåter sådana organ som inte omfattas av några föreskrifter om bevarande och vård av arkiv att behandla känsliga personuppgifter för arkivändamål av allmänt intresse.

Enligt *tredje stycket* får den myndighet som regeringen bestämmer även genom förvaltningsbeslut tillåta ett enskilt organ som inte omfattas av arkivlagstiftningen att behandla känsliga personuppgifter. Bestämmelsen kan bland annat aktualiseras i samband med föreskrifter eller beslut enligt 2 kap. 5 §, om en enskild arkivinstitution samlar in känsliga personuppgifter för arkivändamål av allmänt

intresse. Bestämmelsen kan också tillämpas för att säkerställa att vissa andra enskilda organ ska kunna vidarebehandla känsliga personuppgifter för sådana ändamål, utan samtycke från den registrerade. Ett beslut som tillåter behandling av känsliga personuppgifter för arkivändamål av allmänt intresse förutsätter att den personuppgiftsansvarige vidtar lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen. Dessutom krävs som vid all personuppgiftsbehandling att behandlingen som sådan vilar på rättslig grund eller utgör en tillåten vidarebehandling.

7 § Känsliga personuppgifter får med stöd av artikel 9.2 j i dataskyddsförordningen behandlas om behandlingen är nödvändig för statistiska ändamål och samhällsintresset av det statistikprojekt där behandlingen ingår klart väger över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan innebära.

Paragrafen avser behandling av känsliga personuppgifter för statistiska ändamål och motsvarar 19 § andra stycket PUL. Övervägandena finns i avsnitt 14.5.3.

Bestämmelsen, som har sin grund i artikel 9.2 j i dataskyddsförordningen, utgör ett undantag från förordningens förbud mot att behandla känsliga personuppgifter. För att bestämmelsen över huvud taget ska aktualiseras krävs att insamlingen av personuppgifter är tillåten med stöd av någon av de rättsliga grunderna i artikel 6.1 i dataskyddsförordningen eller att behandlingen utgör en tillåten vidarebehandling av för andra ändamål insamlade personuppgifter.

8 § Regeringen får meddela föreskrifter om ytterligare undantag från förbudet att behandla känsliga personuppgifter i artikel 9.1 i dataskyddsförordningen om det behövs med hänsyn till ett viktigt allmänt intresse.

Paragrafen innehåller ett bemyndigande för regeringen att meddela föreskrifter om ytterligare undantag från förbudet att behandla känsliga personuppgifter. Paragrafen motsvarar delvis 20 § PUL. Övervägandena finns i avsnitt 10.6.2.

Undantag med stöd av bemyndigandet ska vara förenade med skyddsåtgärder i enlighet med dataskyddsförordningens krav.

9 § Personuppgifter som rör fällande domar i brottmål, lagöverträdelser som innefattar brott eller straffprocessuella tvångsmedel får enligt artikel 10 i dataskyddsförordningen behandlas av myndigheter.

Paragrafen avser myndigheters behandling av personuppgifter som rör lagöverträdelser. Paragrafen motsvarar delvis 21 § första stycket PUL. Övervägandena finns i avsnitt 11.4.

Bestämmelsen införlivar delvis första ledet i förordningens artikel 10 i svensk rätt genom att det tydliggörs att myndigheter får behandla sådana uppgifter om lagöverträdelser som avses i artikeln.

Begreppet lagöverträdelser som innefattar brott är detsamma som i personuppgiftslagen. I avvaktan på klargörande EU-rättslig praxis omfattas därför även fortsättningsvis uppgifter om misstankar om brott i viss utsträckning. Faktiska iakttagelser om en persons handlande omfattas normalt sett inte.

10 § Den myndighet som regeringen bestämmer får i enskilda fall besluta att andra än myndigheter får behandla sådana uppgifter som avses i 9 §.

Paragrafen avser enskilda organs behandling av personuppgifter som rör lagöverträdelser. Paragrafen motsvarar delvis 21 § fjärde stycket PUL. Övervägandena finns i avsnitt 11.4.

Bestämmelsen har sin grund i artikel 10 i dataskyddsförordningen, som anger att behandling av uppgifter som rör lagöverträdelser m.m. får utföras under kontroll av en myndighet. Bestämmelsen innebär att den myndighet som regeringen bestämmer kan meddela särskilda beslut om att tillåta sådan behandling i enskilda fall. Sådana beslut bör förenas med villkor såsom återkallelseförbehåll, tidsbegränsningar eller krav på återrapportering, för att på så sätt uppfylla förordningens krav på att behandlingen ska ske under kontroll av en myndighet. Beslut som tillåter behandling av uppgifter om lagöverträdelser i enskilda fall bör dock meddelas endast om intresset av sådan behandling väger tyngre än de registrerades intresse av att behandling inte sker.

11 § Behandling av sådana personuppgifter som avses i 9 § får ske om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om bevarande och vård av arkiv.

Paragrafen avser behandling av personuppgifter som rör lagöverträdelser när behandlingen sker för arkivändamål av allmänt intresse. Paragrafen saknar direkt motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 14.4.3.

Bestämmelsen har sin grund i artikel 10 i dataskyddsförordningen och kompletterar 9 § i fråga om sådan behandling av personuppgifter om lagöverträdelser för arkivändamål av allmänt intresse som utförs av andra än myndigheter.

För att andra än myndigheter ska få behandla personuppgifter om lagöverträdelser för arkivändamål av allmänt intresse med stöd av denna bestämmelse krävs att behandlingen sker som en följd av de skyldigheter att bevara och vårda handlingar som anges i föreskrifter. Detta krav gäller oavsett om personuppgifterna samlas in för arkivändamål av allmänt intresse eller om uppgifter som samlats in för andra ändamål vidarebehandlas för arkivändamål av allmänt intresse. På generell nivå anges sådana skyldigheter i arkivlagen, arkivförordningen samt i Riksarkivets och andra arkivmyndigheters föreskrifter. Det utrymme för behandling av personuppgifter om lagöverträdelser för arkivändamål av allmänt intresse som bestämmelsen ger är därmed i första hand tillgängligt för de organ som omfattas av arkivlagstiftningen. Bestämmelsen medför, tillsammans med 6 § första stycket, att dataskyddsförordningen och lagen inte hindrar att ett enskilt organ som omfattas av offentlighetsprincipen arkiverar och bevarar allmänna handlingar.

12 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om i vilka fall andra än myndigheter får behandla sådana personuppgifter som avses i 9 §.

Paragrafen innehåller ett bemyndigande som motsvarar 21 § tredje stycket PUL. Övervägandena finns i avsnitt 11.4.

Bestämmelsen har stöd i förordningens artikel 10, och innebär att regeringen eller den myndighet som regeringen bestämmer kan tillåta behandling av sådana uppgifter om lagöverträdelser och liknande uppgifter som avses i 9 § i föreskriftsform. Sådana generella föreskrifter kan exempelvis reglera behandling på vissa områden eller för vissa ändamål. Ett krav enligt dataskyddsförordningen är dock att

föreskrifter bara får meddelas om lämpliga skyddsåtgärder för de registrerades grundläggande rättigheter och friheter iakttas.

13 § Uppgifter om personnummer eller samordningsnummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Paragrafen reglerar när personnummer och samordningsnummer får behandlas utan samtycke och motsvarar 22 § PUL. Övervägandena finns i avsnitt 12.4.

Bestämmelsen, som har sin grund i artikel 87 i dataskyddsförordningen, innebär att en intresseavvägning mellan behovet av behandlingen och de integritetsrisker som den innebär ska göras. Omständigheter som bör tillmätas betydelse vid intresseavvägningen är exempelvis om det eftersträvade syftet med behandlingen hade kunnat uppnås på annat sätt, behandlingens omfattning och om den förutsätter samkörning av register.

14 § Regeringen får meddela ytterligare föreskrifter om i vilka fall behandling av personnummer och samordningsnummer är tillåten.

Paragrafen innehåller ett bemyndigande för regeringen att meddela föreskrifter som tillåter behandling av personnummer och samordningsnummer i andra fall än enligt 13 §. Sådana föreskrifter får dock bara meddelas om dataskyddsförordningens krav på lämpliga skyddsåtgärder för de registrerades grundläggande rättigheter och friheter iakttas. Bestämmelsen motsvarar delvis 50 § c PUL. Övervägandena finns i avsnitt 12.4. Bestämmelsen har sin grund i artikel 87 i dataskyddsförordningen.

4 kap. Användningsbegränsningar

1 § Personuppgifter som behandlas enbart för arkivändamål av allmänt intresse får inte användas för att vidta åtgärder i fråga om den registrerade, annat än om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen.

Begränsningen i första stycket hindrar dock inte myndigheter från att använda personuppgifter som finns i allmänna handlingar.

Paragrafen avser användning av arkiverade personuppgifter och motsvarar delvis 9 § fjärde stycket PUL och delvis 8 § andra stycket andra meningen PUL. Övervägandena finns i avsnitt 14.4.4.

Första stycket, som har sin grund i artikel 9.2 j i dataskyddsförordningen, utgör en sådan lämplig och särskild åtgärd som krävs enligt förordningen för att säkerställa den registrerades grundläggande rättigheter och intressen. Bestämmelsen förhindrar att personuppgifter som finns hos den personuppgiftsansvarige enbart för arkivändamål av allmänt intresse används för att vidta åtgärder rörande den registrerade, om det inte finns synnerliga skäl med hänsyn till den registrerades vitala intressen. Begränsningen gäller alla typer av personuppgifter och inte bara känsliga sådana. För att bestämmelsen överhuvudtaget ska aktualiseras krävs att den aktuella användningen är förenlig med det ändamål för vilket uppgifterna ursprungligen samlades in. Bestämmelsen kan alltså inte tillämpas till stöd för en vidarebehandling som i sig är otillåten.

Andra stycket innebär att användningsbegränsningen i första stycket inte gäller för myndigheters användning av personuppgifter i allmänna handlingar. I 1 kap. 5 § anges att vissa andra organ ska jämnställas med myndigheter vid tillämpningen av denna bestämmelse.

2 § Personuppgifter som behandlas enbart för statistiska ändamål får inte användas för att vidta åtgärder i fråga om den registrerade, annat än om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen.

Paragrafen avser användning av statistikuppgifter och motsvarar delvis 9 § fjärde stycket PUL. Övervägandena finns i avsnitt 14.5.4.

Bestämmelsen, som har sin grund i artikel 9.2 j i dataskyddsförordningen, utgör en sådan lämplig och särskild åtgärd som krävs enligt förordningen för att säkerställa den registrerades grundläggande rättigheter och intressen. Bestämmelsen förhindrar att personuppgifter som finns hos den personuppgiftsansvarige enbart för statistiska ändamål används för att vidta åtgärder rörande den registrerade, om det inte finns synnerliga skäl med hänsyn till den

registrerades vitala intressen. Begränsningen gäller alla typer av personuppgifter och inte bara känsliga sådana. För att bestämmelsen överhuvudtaget ska aktualiseras krävs att den aktuella användningen är förenlig med det ändamål för vilket uppgifterna ursprungligen samlades in. Bestämmelsen kan alltså inte tillämpas till stöd för en vidarebehandling som i sig är otillåten. Det bör vidare noteras att bestämmelsen utgör en begränsning även av myndigheters möjligheter att använda statistikuppgifter för att vidta åtgärder i fråga om den registrerade.

5 kap. Begränsningar av vissa rättigheter och skyldigheter

1 § Den registrerades rätt till information och tillgång till personuppgifter enligt artiklarna 13–15 i dataskyddsförordningen gäller inte sådana uppgifter som den personuppgiftsansvarige inte får lämna ut till den registrerade enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning.

Om den personuppgiftsansvarige inte är en myndighet gäller undantaget i första stycket även för uppgifter som hos en myndighet skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen (2009:400).

Paragrafen föreskriver undantag från den personuppgiftsansvariges informationsskyldighet och motsvarar i sak 27 § PUL. Övervägandena finns i avsnitt 13.4.1.

Bestämmelsen har stöd i artikel 23 i dataskyddsförordningen. Första stycket innebär att sådan sekretess eller tystnadsplikt gentemot den registrerade som har stöd i författning har företräde framför rätten att få information och tillgång till de personuppgifter som behandlas.

Andra stycket innebär att en personuppgiftsansvarig som inte omfattas av offentlighets- och sekretesslagens tillämpningsområde får vägra att lämna ut information till den registrerade, om en bestämmelse i den lagen hade hindrat utlämnande till den registrerade om den personuppgiftsansvarige hade varit en myndighet.

2 § Bestämmelsen om den registrerades rätt till tillgång till personuppgifter i artikel 15 i dataskyddsförordningen gäller inte personupp-

gifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande.

Undantaget i första stycket gäller inte om personuppgifterna

- 1. har lämnats ut till tredje part,*
- 2. behandlas enbart för arkivändamål av allmänt intresse eller statistiska ändamål, eller*
- 3. har behandlats under längre tid än ett år i löpande text som inte fått sin slutliga utformning.*

Paragrafen föreskriver undantag från den personuppgiftsansvariges skyldighet att på den registrerades begäran lämna s.k. registerutdrag. Bestämmelsen motsvarar i sak 26 § tredje stycket PUL. Övervägandena finns i avsnitt 13.4.2.

Bestämmelsen i *första stycket*, som har stöd i artikel 23 i dataskyddsförordningen, innebär att den personuppgiftsansvarige inte behöver söka fram och lämna ut personuppgifter som finns i arbetsmaterial i form av löpande text. Med löpande text avses information som inte har strukturerats så att sökning av personuppgifter underlättas. Med text som inte har fått sin slutliga utformning avses koncept och utkast och liknande. Text som är avsedd att tid efter annan ändras eller kompletteras och således aldrig kommer att få någon slutlig utformning omfattas inte av undantaget. Med text som utgör minnesanteckning avses promemorior och liknande som har kommit till bara för att bereda något slags ärende.

Undantaget begränsas genom *andra stycket*. Begränsningen i *punkt 1* innebär att rätten till registerutdrag ändå gäller, om den handling där personuppgifterna förekommer har lämnats ut till någon tredje part. *Punkt 2* innebär bland annat att rätten till registerutdrag omfattar personuppgifter i sådana utkast eller minnesanteckningar som har tagits om hand för arkivering. Med behandling för arkivändamål av allmänt intresse eller statistiska ändamål avses detsamma som i dataskyddsförordningen. Slutligen innebär *punkt 3* att personuppgifter som förekommer i löpande text som inte har fått sin slutliga utformning ska lämnas ut, om behandlingen har pågått under längre tid än ett år. Minnesanteckningar, som normalt får sin slutliga utformning i samband med att de förs, omfattas däremot inte av punkt 3. Personuppgifter som förekommer i sådana handlingar behöver således inte lämnas ut, även om behandlingen pågått i mer än ett år, om inte någon av punkterna 1 eller 2 är tillämpliga.

3 § Regeringen får meddela föreskrifter om ytterligare begränsningar av vissa rättigheter och skyldigheter enligt artikel 23 i dataskyddsförordningen.

Paragrafen föreskriver ett bemyndigande för regeringen att meddela föreskrifter med stöd av artikel 23 i dataskyddsförordningen. Bestämmelsen motsvarar i sak 8 a § PUL. Övervägandena finns i avsnitt 13.4.4.

6 kap. Tillsynsmyndighetens handläggning och beslut

1 § De befogenheter som tillsynsmyndigheten har enligt artikel 58.1, 58.2 och 58.3 i dataskyddsförordningen gäller även vid tillsyn över efterlevnaden av bestämmelserna i denna lag och andra författningar som kompletterar dataskyddsförordningen.

Paragrafen avser tillsynsmyndighetens befogenheter och saknar direkt motsvarighet i personuppgiftslagen, men fyller i sak samma funktion som 2a § andra stycket förordningen (2007:975) med instruktion för Datainspektionen. Övervägandena finns i avsnitt 19.5.3.

Bestämmelsen, som införs mot bakgrund av artiklarna 55–58 i dataskyddsförordningen, innebär att de tillsynsåtgärder som tillsynsmyndigheten kan vidta vid överträdelser av förordningen också kan vidtas vid överträdelser av bestämmelser i svensk rätt som kompletterar förordningen. Detta gäller oavsett om dessa kompletterande bestämmelser om behandling av personuppgifter finns i denna lag eller i sektorsspecifika författningar. Det bör dock noteras att den befogenhet som tillsynsmyndigheten har enligt artikel 58.2 i, när det gäller att påföra administrativa sanktionsavgifter, hänvisar till artikel 83, som i sin tur innehåller en uttömmande uppräkningslista av vilka överträdelser som föranleder sanktionsavgifter. Av denna uppräkningslista framgår motsatsvis att sanktionsavgifter kan påföras vid överträdelser av nationella bestämmelser endast om dessa bestämmelser antagits på grundval av kapitel IX i dataskyddsförordningen.

2 § Om tillsynsmyndigheten vid handläggningen av ett ärende finner att det finns skäl att ifrågasätta giltigheten av en unionsrättsakt

som påverkar tillämpningen av dataskyddsförordningen i ärendet, får tillsynsmyndigheten hos allmän förvaltningsdomstol ansöka om att en åtgärd enligt artikel 58.2 i dataskyddsförordningen ska vidtas.

Ansökan ska göras hos den förvaltningsrätt som är behörig att pröva ett överklagande av tillsynsmyndighetens beslut.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen avser tillsynsmyndighetens möjlighet att anhängiggöra ett mål i domstol om behandling av personuppgifter. Paragrafen saknar motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 19.5.3.

Bestämmelsen i *första stycket*, som har sin grund i artikel 58.5 i dataskyddsförordningen, innebär att tillsynsmyndigheten, om den anser att det finns skäl att ifrågasätta om en unionsrättsakt som påverkar tillämpningen av dataskyddsförordningen är giltig, kan avstå från att själv fatta beslut om korrigerande tillsynsåtgärder enligt artikel 58.2 och i stället ansöka hos förvaltningsrätten om att åtgärden ska beslutas. Bestämmelsen kan aktualiseras vid normkonflikt mellan dataskyddsförordningen och andra unionsrättsakter, t.ex. om ett kommissionsbeslut kräver eller förhindrar att en tillsynsåtgärd ska vidtas, men en sådan tillämpning skulle stå i strid med förordningen eller fördragen. Tillsynsmyndigheten kan i en sådan situation inte själv lösa normkonflikten genom att sätta någon av rättsakterna åt sidan. I stället får myndigheten ansöka hos förvaltningsrätten om att en tillsynsåtgärd ska vidtas. Om domstolen i ett sådant mål delar tillsynsmyndighetens tvivel angående giltigheten av den unionsrättsakt som förhindrar eller kräver att åtgärden vidtas, kan domstolen begära ett förhandsavgörande från EU-domstolen och därigenom få giltigheten prövad innan något beslut om åtgärden fattas.

Enligt *andra stycket* ska ansökan göras hos den förvaltningsrätt som är behörig att pröva överklaganden av tillsynsmyndighetens beslut. Av *tredje stycket* framgår att prövningstillstånd krävs vid överklagande till kammarrätten.

3 § Innan tillsynsmyndigheten fattar ett beslut som avses i artikel 58.2 i dataskyddsförordningen, ska den som beslutet gäller ges tillfälle att inom en bestämd tid yttra sig över allt material av betydelse för beslutet, om det inte är uppenbart obehövligt.

Om saken är brådskande får myndigheten, i avvaktan på yttrandet, besluta att behandlingen av personuppgifter tillfälligt ska begränsas eller förbjudas i enlighet med artikel 58.2 f i dataskyddsförordningen. Det tillfälliga beslutet ska omprövas, när tiden för yttrande har gått ut.

Paragrafen reglerar tillsynsmyndighetens kommunikationsplikt. Paragrafen motsvarar delvis 46 § första stycket PUL. Övervägandena finns i avsnitt 19.5.3.

Bestämmelsen införs mot bakgrund av artikel 58.4 i dataskyddsförordningen. Av *första stycket* i paragrafen följer att tillsynsmyndigheten – innan den fattar vissa slags beslut – ska underrätta den som beslutet gäller om allt material av betydelse för beslutet och ge denne tillfälle att inom en bestämd tid yttra sig över materialet, om det inte är uppenbart obehövligt. Bestämmelsen gäller sådana beslut som tillsynsmyndigheten meddelar med stöd av de korrigerande befogenheter som föreskrivs i artikel 58.2 i förordningen, oavsett om mottagaren är en enskild eller en myndighet. Avseende andra slags beslut gäller förvaltningslagens allmänna bestämmelser om kommuniceringsskyldighet.

Kravet på kommunikation omfattar enbart sådant material som utgör underlag för beslutet, inte varje uppgift som har tillförts ärendet utifrån. Sådant material som helt saknar relevans för ett beslut i ett ärende omfattas alltså inte av kravet på kommunikation. Med material av betydelse avses sådana omständigheter eller uppgifter i materialet som påverkar tillsynsmyndighetens ställningstagande i den fråga som beslutet gäller. Det är alltså inte ett förslag till beslut som ska kommuniceras. Hur lång svarsfrist som kan anses rimlig och lämplig får avgöras utifrån bland annat materialets omfattning och komplexitet.

Det sista ledet i första stycket innebär en begränsning av huvudregeln för att undvika onödig kommunikation i de fall då detta är uppenbart obehövligt. Regeln ska tolkas snävt och är tillämplig enbart i sådana fall där behovet av kommunikation – sett ur mottagarens perspektiv – är mindre framträdande eller helt saknas. Det måste alltså stå klart för tillsynsmyndigheten att åtgärden inte kan tillföra något i det aktuella ärendet. Ett tänkbart exempel kan vara att det är mottagaren själv som har lämnat uppgifterna. Närmare praxis om när det är uppenbart obehövligt med kommunikation får utvecklas i rättstillämpningen.

Enligt *andra stycket* får tillsynsmyndigheten i vissa fall besluta om begränsning av eller förbud mot behandling av personuppgifter redan innan tiden för yttrande har löpt ut. En förutsättning för detta är att saken är brådskande. Ett omedelbart ingripande ska alltså vara motiverat av en överhängande risk för allvarlig kränkning av enskildas personliga integritet. Kommunikationsplikten gäller även i en sådan situation, men tillsynsmyndigheten behöver inte invänta att den som beslutet gäller kommer in med yttrandet eller avvakta till den tidpunkt då tiden för yttrande går ut innan beslut fattas. Tillsynsmyndighetens beslut ska dock vara tillfälligt och ska omprövas när tiden för yttrande har gått ut.

4 § Ett beslut som avses i 3 § första stycket ska delges, om det inte är uppenbart obehövligt. Delgivning enligt 34–37 §§ delgivningslagen (2010:1932) får användas endast om det finns särskild anledning att anta att mottagaren har avvikit eller på annat sätt håller sig undan.

Paragrafen reglerar när en underrättelse om ett beslut enligt artikel 58.2 i dataskyddsförordningen ska ske genom delgivning. Bestämmelsen motsvarar delvis 46 § andra stycket PUL. Övervägandena finns i avsnitt 19.5.3.

Bestämmelsen införs mot bakgrund av artikel 58.4 i dataskyddsförordningen. Att beslut ska delges innebär att myndigheten ska använda sig av de metoder för delgivning som regleras i delgivningslagen för att säkerställa att den som beslutet gäller får del av underrättelsen. Vissa delgivningsmetoder får dock bara användas under särskilda omständigheter. Om delgivning är uppenbart obehövligt, eller om beslutet inte grundar sig på befogenheterna i artikel 58.2 i förordningen, gäller förvaltningslagens generella bestämmelser om att myndigheten själv bestämmer hur en underrättelse om ett beslut ska gå till. Som exempel på när det kan anses vara uppenbart obehövligt att delge ett beslut kan nämnas att det som regel är uppenbart obehövligt att delge beslut enligt delgivningslagen när mottagaren är en myndighet. Däremot kan det aldrig anses uppenbart obehövligt att delge beslut om administrativa sanktionsavgifter. Närmare praxis om när det är uppenbart obehövligt med delgivning får utvecklas i rättstillämpningen.

5 § Om tillsynsmyndigheten inte inom tre månader från den dag då ett klagomål kom in till myndigheten har behandlat klagomålet, ska tillsynsmyndigheten på skriftlig begäran av den registrerade antingen lämna besked i frågan om myndigheten avser att utöva tillsyn med anledning av klagomålet, eller i ett särskilt beslut avslå begäran om besked.

Besked eller beslut enligt första stycket ska meddelas inom två veckor från den dag då begäran om besked kom in till myndigheten.

Om tillsynsmyndigheten har avslagit en begäran om besked enligt första stycket, har den registrerade inte rätt till ett nytt besked i ärendet förrän tidigast tre månader efter det att myndighetens beslut meddelades.

I paragrafen finns bestämmelser om den registrerades rätt att på begäran få besked om tillsynsmyndighetens handläggning av ett klagomål. Paragrafen har inte någon motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 19.4.3.

Bestämmelsen har, liksom 8 kap. 3 §, sin grund i artikel 78.2 i dataskyddsförordningen. Av paragrafens *första stycke* följer att en registrerad som har lämnat in ett klagomål till tillsynsmyndigheten skriftligen får begära besked i ärendet, om tillsynsmyndigheten inte inom tre månader har behandlat klagomålet. Tillsynsmyndigheten ska då antingen lämna besked i frågan om myndigheten avser att utöva tillsyn med anledning av klagomålet eller i ett särskilt beslut avslå den registrerades begäran om besked.

En begäran om besked ska vara skriftlig, men skriftlighetskravet är teknikoberoende. Det förutsätter endast att framställningen görs i en form som är läsbar för myndigheten. Det kan ske både i elektronisk form och på papper. Om en begäran görs muntligen – per telefon eller vid en personlig inställelse på myndigheten – är bestämmelsen alltså inte tillämplig. I ett sådant fall bör myndigheten dock, i enlighet med bestämmelserna i förvaltningslagen om myndigheternas service-skyldighet, upplysa parten om formkravet.

Det är bara framställningar som görs sedan minst tre månader har förflutit efter det att klagomålet lämnades in som måste beaktas vid tillämpningen av denna bestämmelse. Om en begäran om besked i ärendet görs innan denna spärrtid har passerat behöver tillsynsmyndigheten alltså inte ta ställning till begäran på det sätt som anges i bestämmelsen. Begäran kan då i stället avvisas.

Ett besked om att tillsynsmyndigheten avser att utöva tillsyn behöver inte innebära att tillsynsmyndigheten kommer att vidta någon av de korrigerande åtgärderna i artikel 58.2 i förordningen. Tillsynsmyndigheten utövar tillsyn även när den vidtar sådana utredningsåtgärder som avses i artikel 58.1, som till exempel att beordra den personuppgiftsansvarige att lämna information rörande behandlingen av personuppgifter. Tillsynsmyndighetens möjlighet att, i stället för att lämna besked, avslå den registrerades begäran ska användas restriktivt. Beslut om avslag bör fattas endast i de fall då ytterligare handläggningstid är motiverad av sakliga skäl som är kopplade till det aktuella ärendet. En sådan situation kan till exempel uppstå om samma sakfråga som den som klagomålet gäller, men rörande en annan personuppgiftsansvarig, är föremål för domstolsprövning och utgången i målet är oviss. Tillsynsmyndighetens beslut att avslå en begäran om besked får överklagas av den registrerade enligt 8 kap. 3 §.

Av *andra stycket* följer att tillsynsmyndigheten inom två veckor från den dag då begäran kom in antingen ska lämna besked eller i ett särskilt beslut avslå begäran. Myndigheten kan alltså inte välja att förhålla sig helt passiv. Eftersom beslutet ska kunna överklagas är det lämpligt att myndigheten dokumenterar beslutet skriftligt och anger skälen för detta.

Om tillsynsmyndigheten har avslagit en begäran om besked följer det av *tredje stycket* att den registrerade inte kan påkalla ett nytt besked i samma ärende förrän efter ytterligare tre månader. Om en förnyad begäran kommer in till tillsynsmyndigheten innan denna spärrtid har förflutit, ska tillsynsmyndigheten avvisa den nya begäran. Ett sådant avvisningsbeslut får inte överklagas enligt 8 kap. 3 §, jfr 8 kap. 5 §.

7 kap. Administrativa sanktionsavgifter

1 § Sanktionsavgift får tas ut av en myndighet vid överträdelser som avses i artikel 83.4, 83.5 och 83.6 i dataskyddsförordningen, varvid artikel 83.1, 83.2 och 83.3 i förordningen ska tillämpas.

Vid överträdelser som avses i artikel 83.4 i dataskyddsförordningen ska avgiften bestämmas till högst 10 000 000 kronor och annars till högst 20 000 000 kronor.

Paragrafen innebär att sanktionsavgifter enligt förordningen kan tas ut även av myndigheter, och anger de övre beloppsgränser som gäller i sådana fall. Paragrafen har ingen motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 18.5.3.

Bestämmelserna i paragrafen har sin grund i artikel 83.7 i dataskyddsförordningen, enligt vilken varje medlemsstat får reglera om och i vilken utsträckning det ska vara möjligt att besluta om sanktionsavgifter mot offentliga myndigheter och organ.

Bestämmelsen i *första stycket* innebär att den reglering avseende påförande av sanktionsavgifter som finns i artikel 83.1–3 i förordningen gäller vid beslut även mot myndigheter. Avgiftens storlek i det enskilda fallet ska alltså bestämmas med beaktande av vad som stadgas där, men inom de beloppsmässiga ramar som framgår av bestämmelsen i *andra stycket*.

2 § Sanktionsavgift får tas ut vid överträdelse av artikel 10 i dataskyddsförordningen, varvid artikel 83.1, 83.2 och 83.3 i förordningen ska tillämpas. Avgiftens storlek ska bestämmas med tillämpning av artikel 83.5 i förordningen.

Paragrafen, som innebär att administrativa sanktionsavgifter kan påföras även avseende överträdelse mot förordningens reglering av behandling av uppgifter om lagöverträdelse m.m. i artikel 10, saknar motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 18.6.4.

Det framgår av artikel 83.4–6 i dataskyddsförordningen att någon möjlighet att påföra sanktionsavgifter vid överträdelse mot artikel 10 inte följer direkt av förordningen. Bestämmelsen medför att samma reglering för sanktionsavgifter ska gälla som enligt förordningen, och att det är den övre beloppsgränsen enligt artikel 83.5 i förordningen som gäller för sådana överträdelse.

Det bör noteras att enligt artikel 10 får myndigheter behandla personuppgifter som rör lagöverträdelse. Det blir därmed inte aktuellt att ta ut sanktionsavgift av en myndighet enligt denna paragraf.

3 § Sanktionsavgift får inte beslutas, om den som avgiften ska tas ut av inte har fått tillfälle att yttra sig enligt 6 kap. 3 § inom fem år från den dag då överträdelset ägde rum.

Paragrafen, som saknar motsvarighet i personuppgiftslagen, innebär att det finns en bortre tidsgräns för när sanktionsavgift får beslutas. Övervägandena finns i avsnitt 19.5.3.

Bestämmelsen innebär att om kommunikation enligt 6 kap. 3 § inte har skett mot den som ska påföras avgiften inom fem år från överträdelserna, får den inte beivras. Bevisbördan för att kommunikation har skett åligger tillsynsmyndigheten, vilket i praktiken innebär att underrättelsen bör delges.

Tidsfristen börjar löpa när behandlingen upphör. Så länge otillåten eller felaktig behandling pågår är det fråga om en pågående överträdelse. Den i paragrafen angivna tiden förskjuts då framåt så länge behandlingen pågår.

4 § En sanktionsavgift som beslutats enligt dataskyddsförordningen eller denna lag tillfaller staten.

Paragrafen, som saknar motsvarighet i personuppgiftslagen, föreskriver att sanktionsavgifter som tas ut enligt dataskyddsförordningen eller denna lag ska tillfalla staten. Övervägandena finns i avsnitt 18.7.1.

8 kap. Skadestånd och rättsmedel

1 § Rätten till ersättning enligt artikel 82 i dataskyddsförordningen gäller även vid överträdelser av bestämmelser i denna lag och andra författningar som kompletterar dataskyddsförordningen.

Paragrafen avser rätten till skadestånd vid överträdelser av bestämmelser om behandling av personuppgifter som kompletterar dataskyddsförordningen. Bestämmelsen saknar motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 19.3.3.

Bestämmelsen, som har sin grund i förordningens artikel 82 och skäl 146, upplyser om att den rätt till ersättning som regleras i dataskyddsförordningen även gäller vid överträdelser av de bestämmelser om behandling av personuppgifter som finns i lagen och i andra författningar som kompletterar dataskyddsförordningen.

2 § Beslut enligt artiklarna 12.5, 15–19 eller 21 i dataskyddsförordningen som har meddelats av en myndighet i egenskap av personuppgiftsansvarig får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Första stycket gäller inte beslut av riksdagen, regeringen, Högsta domstolen, Högsta förvaltningsdomstolen eller riksdagens ombudsmän.

Paragrafen reglerar rätten att överklaga beslut som en personuppgiftsansvarig myndighet meddelar med anledning av att en registrerad utövar sina rättigheter enligt dataskyddsförordningen. Paragrafen, som har sin grund i allmänna förvaltningsrättsliga principer, motsvarar i sak 52 § PUL. Övervägandena finns i avsnitt 19.3.3.

3 § Tillsynsmyndighetens beslut att avslå en begäran om besked enligt 6 kap. 5 § får överklagas till allmän förvaltningsdomstol.

Om domstolen bifaller överklagandet, ska den förelägga tillsynsmyndigheten att inom en bestämd tid lämna besked till den registrerade i frågan om tillsyn kommer att utövas.

Domstolens beslut får inte överklagas.

Paragrafen reglerar rätten till dröjsmålstalan i domstol avseende tillsynsmyndighetens handläggning av ett klagomål. Bestämmelsen saknar motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 19.7.3.

Bestämmelsen har, liksom 6 kap. 5 §, sin grund i artikel 78.2 i dataskyddsförordningen. Av *första stycket* i paragrafen följer att tillsynsmyndighetens beslut att avslå en begäran om besked rörande handläggningen av ett klagomål får överklagas till förvaltningsrätten. Beslut att avvisa en begäran om besked, till exempel på grund av att spärrtiden enligt 6 kap. 5 § första eller tredje stycket inte har löpt ut, får däremot inte överklagas.

I *andra stycket* anges att domstolen, om den bifaller överklagandet, ska förelägga tillsynsmyndigheten att lämna besked i ärendet. Domstolen ska alltså inte pröva om klagomålet till tillsynsmyndigheten är befogat, utan endast ta ställning till om handläggningstiden hos tillsynsmyndigheten är berättigad och motiverad.

Domstolens beslut med anledning av den registrerades dröjsmålstalan får enligt *tredje stycket* inte överklagas.

4 § Tillsynsmyndighetens beslut enligt dataskyddsförordningen och enligt 7 kap. 1 och 2 §§ denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen avser rätten att överklaga tillsynsmyndighetens beslut enligt dataskyddsförordningen samt om administrativa sanktionsavgifter enligt lagen. Bestämmelsen har sin grund i artikel 78.1 i dataskyddsförordningen och motsvarar 51 § och 53 § andra stycket PUL. Övervägandena finns i avsnitt 19.7.3.

5 § Beslut enligt 2 kap. 5 § andra stycket, 3 kap. 6 § tredje stycket och 3 kap. 10 § denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen avser rätten att överklaga sådana beslut i enskilda fall som den myndighet som regeringen bestämmer meddelar avseende behandling av personuppgifter för arkivändamål av allmänt intresse samt avseende behandling av personuppgifter som rör lagöverträdelser. Bestämmelsen har sin grund i allmänna förvaltningsrättsliga principer. Övervägandena finns i avsnitt 19.8.

6 § Andra beslut enligt denna lag än de som avses i 2–5 §§ och 6 kap. 2 § får inte överklagas.

Paragrafen avser överklagande och motsvarar i sak 53 § PUL. Övervägandena finns i avsnitt 19.8.

Bestämmelsen innebär att tillsynsmyndighetens beslut att avvisa eller avskriva en begäran om besked enligt 6 kap. 5 § inte får överklagas. Beslut att meddela föreskrifter med stöd av bemyndigandena i lagen får inte heller överklagas.

22.2 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

10 kap.

27 § Utöver vad som följer av 2, 3, 5 och 15–26 §§ får en sekretessbelagd uppgift lämnas till en myndighet, om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

Första stycket gäller inte i fråga om sekretess enligt 24 kap. 2 a och 8 §§, 25 kap. 1–8 §§, 26 kap. 1–6 §§, 29 kap. 1 och 2 §§, 31 kap. 1 § första stycket, 2 och 12 §§, 33 kap. 2 §, 36 kap. 3 § samt 40 kap. 2 och 5 §§.

Första stycket gäller inte heller om utlämnandet strider mot lag eller förordning.

Paragrafen behandlas i avsnitt 17.6.2. Den reglerar utlämnande av uppgifter som omfattas av sekretess mellan myndigheter i fall då det saknas uttryckliga sekretessbrytande regler. Ändringen innebär att tredje styckets hänvisning till föreskrifter som har meddelats med stöd av personuppgiftslagen stryks.

Tredje styckets hänvisning till lag eller förordning innefattar också EU-förordningar. Detta medför att ett utlämnande till annan myndighet som strider mot dataskyddsförordningen eller dataskyddslagen inte kan ske med stöd av generalklausulen.

21 kap.

Behandling i strid med *dataskyddsregleringen*

7 § Sekretess gäller för personuppgift, om det kan antas att *uppgiften efter ett utlämnande kommer att behandlas i strid med Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), i den ursprungliga lydelsen, eller lagen (2018:xx) med kompletterande bestämmelser till EU:s dataskyddsförordning.*

Paragrafen behandlas i avsnitt 17.5.2. Ändringen innebär dels ett förtydligande av att prövningen enligt denna bestämmelse gäller den behandling som kommer att ske efter ett eventuellt utlämnande, dels att hänvisningen till personuppgiftslagen ersätts med en hänvisning till dataskyddsförordningen och dataskyddslagen. En konsekvens av att hänvisningen inte enbart avser nationell rätt är att utlämnanden till utländska mottagare som omfattas av dataskyddsförordningens tillämpningsområde också omfattas av sekretessbestämmelsen. I övrigt är äldre förarbetsuttalanden relevanta även fortsättningsvis.

Hänvisningen till dataskyddsförordningen i denna paragraf är statisk, dvs. avser den ursprungliga lydelsen av förordningen.

40 kap.

5 § Sekretess gäller för uppgift om en enskilds personliga eller ekonomiska förhållanden i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning av sådana personuppgifter som avses i artikel 4.1 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Paragrafen behandlas i avsnitt 17.7.2. Ändringen innebär att hänvisningen till personuppgiftslagen ersätts med en hänvisning till dataskyddsförordningen.

Hänvisningen till förordningen medför att förordningens definition av personuppgifter blir avgörande för sekretessens räckvidd. I övrigt är tidigare förarbetsuttalanden relevanta även fortsättningsvis. Av dessa framgår följande. Sekretessen gäller hos en myndighet som behandlar personuppgifter såväl då det är fråga om bearbetning eller lagring för enskildas räkning som då det gäller bearbetning eller lagring av en annan myndighets personuppgifter. Med teknisk bearbetning avses t.ex. att myndigheten scannar in text på papper för att lagra elektroniskt. Teknisk lagring avser alla former av lagring som kräver särskilda tekniska anordningar, t.ex. lagring av information på hårdisk eller i molntjänster. Personuppgifter som förvaras hos en arkiv-

myndighet anses normalt inte tekniskt lagrade för någon annans räkning.

Sekretessen enligt paragrafen är absolut. Tryckfrihetsförordningens reglering i 2 kap. 10 § första stycket innebär dock att handlingar som förvaras hos en myndighet endast som ett led i teknisk bearbetning eller lagring inte är att anse som allmänna handlingar där. Det innebär i sin tur att bestämmelsen i 40 kap. 5 § OSL inte har någon praktisk betydelse för utlämnande av uppgifter i allmänna handlingar, utan endast fyller funktionen av en tystnadspliktsbestämmelse som hindrar utlämnande på myndighetens eller befattningshavarens eget initiativ.

Hänvisningen till dataskyddsförordningen i denna paragraf är dynamisk, dvs. avser den vid varje tidpunkt gällande definitionen av personuppgiftsbegreppet i förordningen.

Kommittédirektiv 2016:15

Dataskyddsförordningen

Beslut vid regeringssammanträde den 25 februari 2016

Sammanfattning

Inom kort förväntas EU besluta om en förordning som utgör en ny generell reglering för personuppgiftsbehandling inom EU. En särskild utredare ska föreslå de anpassningar och kompletterande författningsbestämmelser på generell nivå som denna förordning ger anledning till. Syftet är att säkerställa att det finns en ändamålsenlig och välbalanserad kompletterande nationell reglering om personuppgiftsbehandling på plats när förordningen börjar tillämpas.

Utredaren ska bl.a.

- undersöka vilka kompletterande nationella föreskrifter, exempelvis processuella bestämmelser, som förordningen kräver,
- analysera vilka bestämmelser om administrativa sanktionsavgifter och andra sanktioner som Sverige behöver eller bör införa,
- överväga vilka kompletterande bestämmelser om t.ex. behandling av känsliga personuppgifter och personnummer som bör införas i den svenska generella regleringen,
- undersöka om det finns behov av generella bestämmelser för personuppgiftsbehandling utanför EU-rättens tillämpningsområde, och
- lämna sådana författningsförslag som är behövliga och lämpliga.

I uppdraget ingår inte att överväga eller lämna förslag till grundlagsändringar.

Uppdraget ska redovisas senast den 12 maj 2017.

Den nuvarande och den nya regleringen

Dataskyddsdirektivet – den nuvarande EU-regleringen

Den allmänna regleringen om behandling av personuppgifter inom EU finns i dag i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om behandling av det fria flödet av sådana uppgifter (dataskyddsdirektivet). Direktivet syftar till att garantera en hög och i alla medlemsstater likvärdig skyddsnivå när det gäller enskilda personers fri- och rättigheter med avseende på behandling av personuppgifter, samt att främja ett fritt flöde av personuppgifter mellan medlemsstaterna i EU.

Dataskyddsdirektivet gäller inte för behandling av personuppgifter på områden som faller utanför gemenskapsrätten, t.ex. allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område.

Personuppgiftslagen – den nuvarande svenska regleringen

Dataskyddsdirektivet har genomförts i svensk rätt huvudsakligen genom personuppgiftslagen (1998:204), förkortad PUL. Bestämmelserna i personuppgiftslagen har till syfte att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Personuppgiftslagen följer i princip dataskyddsdirektivets struktur och innehåller liksom direktivet bestämmelser om bl.a. personuppgiftsansvar, grundläggande krav för behandling av personuppgifter, information till den registrerade, skadestånd och straff.

Personuppgiftslagen är tillämplig även utanför EU-rättens område och gäller både för myndigheter och enskilda som behandlar personuppgifter. Personuppgiftslagen är samtidigt subsidiär vilket innebär att lagens bestämmelser inte ska tillämpas om det finns avvikande bestämmelser i en annan lag eller förordning. Det finns en stor mängd sådana bestämmelser i s.k. särskilda registerförfattningar som

främst reglerar hur olika myndigheter får behandla personuppgifter, t.ex. studiestödsdatalagen (2009:287) och polisdatalagen (2010:361). Men det finns också sådana bestämmelser i regleringar som primärt har andra syften än att reglera personuppgiftsbehandling, exempelvis i vapenlagen (1996:67) och kreditupplysningslagen (1973:1173).

Personuppgiftslagen kompletteras också av bestämmelser i personuppgiftsförordningen (1998:1191), förkortad PUF, som bl.a. pekar ut Datainspektionen som tillsynsmyndighet enligt lagen. Datainspektionen bemyndigas i förordningen att meddela närmare föreskrifter om bl.a. i vilka fall behandling av personuppgifter är tillåten och vilka krav som ställs på den personuppgiftsansvarige.

Regeringsformen och kravet på lagreglering för viss personuppgiftsbehandling

Sedan den 1 januari 2011 anges i 2 kap. 6 § andra stycket regeringsformen att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Begränsningar av denna fri- och rättighet får enligt 2 kap. 20 § första stycket regeringsformen under vissa förutsättningar göras genom lag. Regleringen i regeringsformen innebär att viss personuppgiftsbehandling måste regleras i lag.

Dataskyddsförordningen – den nya regleringen

Inom kort förväntas Europaparlamentet och rådet fatta beslut om förordningen om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning), nedan dataskyddsförordningen.¹ Förordningen utgör en ny generell reglering för personuppgiftsbehandling inom EU och kommer att ersätta det nuvarande dataskyddsdirektivet. Förordningen ska börja tillämpas två år räknat från den tjugonde dagen efter publicering i Europeiska unionens offi-

¹ Kommittédirektiven utgår från den version av förslaget som finns i dok. 5455/16 av den 28 januari 2016.

ciella tidning. Det huvudsakliga syftet med förordningen är att ytterligare harmonisera och effektivisera skyddet för personuppgifter för att förbättra den inre marknadens funktion och öka enskildas kontroll över sina personuppgifter.

Dataskyddsförordningen baseras till stor del på dataskyddsdirektivets struktur och innehåll men innebär även en rad nyheter såsom en utökad informationsskyldighet, administrativa sanktionsavgifter och inrättandet av Europeiska dataskyddsstyrelsen. Dataskyddsförordningen är direkt tillämplig i medlemsstaterna men både förutsätter och möjliggör kompletterande nationella bestämmelser av olika slag. Det finns t.ex. ett förhållandevis stort utrymme att behålla eller införa särregleringar för sådan personuppgiftsbehandling som är nödvändig för att den personuppgiftsansvarige ska kunna uppfylla en rättslig skyldighet, utföra en arbetsuppgift av allmänt intresse eller behandla uppgifter i samband med myndighetsutövning.

Från dataskyddsförordningens tillämpningsområde undantas behandling av personuppgifter som utgör ett led i en verksamhet som a) inte omfattas av unionsrätten, b) utförs av medlemsstaterna när de utför aktiviteter som omfattas av den gemensamma utrikes- och säkerhetspolitiken, c) utförs av en fysisk person som ett led i verksamhet av privat natur eller som har samband med dennes hushåll eller d) utförs av behöriga myndigheter för ändamålen att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder, inkluderande skydd mot samt förebyggande av hot mot allmän säkerhet. Förordningen gäller inte heller för behandling av personuppgifter som utförs av EU:s institutioner, organ och byråer. Sådan behandling regleras i stället i Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter.

Samtidigt med dataskyddsförordningen förväntas Europaparlamentet och rådet anta direktivet om skyddet av enskilda vid behöriga myndigheters behandling av personuppgifter i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, samt fri rörlighet för sådana uppgifter, nedan ”det nya dataskyddsdirektivet”. Direktivet innehåller särregler för sådan personuppgiftsbehandling som behöriga myndigheter utför i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga

påföljder, inkluderande skydd mot samt förebyggande av hot mot allmän säkerhet. Direktivet ska ersätta det gällande dataskyddsrambeslutet (2008/977/RIF) som reglerar utbyte av personuppgifter mellan medlemsstaterna inom denna sektor. Direktivets tillämpningsområde omfattar till skillnad från rambeslutet emellertid även rent nationell personuppgiftsbehandling på området för brottsbekämpning, brottmålshantering och straffverkställighet. Direktivet ska ha genomförts i svensk rätt senast två år efter att det har trätt i kraft.

Vid vissa myndigheter, bl.a. de allmänna domstolarna, Kriminalvården och Kustbevakningen, kommer personuppgiftsbehandlingen att omfattas av antingen dataskyddsförordningen eller det nya dataskyddsdirektivet beroende på vilket syfte uppgifterna behandlas för. Det gäller även Polismyndigheten som vid sidan av den brottsbekämpande verksamheten t.ex. sköter handräckning och handlägger olika typer av tillståndsärenden. Myndigheter vars kärnverksamhet huvudsakligen omfattas av det nya dataskyddsdirektivets tillämpningsområde kommer också att tillämpa dataskyddsförordningen när de exempelvis överför uppgifter för ändamål utanför direktivets tillämpningsområde.

Vid sidan av den EU-rättsliga dataskyddsregleringen finns Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (CETS 108), den s.k. dataskyddskonventionen. För svensk del har konventionen, som har ett generellt tillämpningsområde, främst betydelse för personuppgiftsbehandling utanför EU-regleringens tillämpningsområde. En översyn av konventionen pågår inom Europarådet.

Uppdraget

Allmänna riktlinjer för uppdraget

Dataskyddsförordningen kommer att utgöra grunden för generell personuppgiftsbehandling inom EU. Detta innebär att personuppgiftslagen och personuppgiftsförordningen, samt Datainspektionens föreskrifter i anslutning till denna reglering, måste upphävas. Det finns samtidigt ett behov av att ta fram en nationell reglering som på ett generellt plan kompletterar förordningen. En sådan kompletterande reglering behöver bl.a. innehålla bestämmelser om sanktioner och om tillsynsmyndigheten. Dataskyddsförordningen lämnar dess-

utom utrymme för kompletterande nationella bestämmelser med ytterligare krav eller undantag i en rad andra frågor.

Med anledning av detta finns det behov av en utredning. Det övergripande uppdraget för utredaren bör vara att föreslå författningsbestämmelser som på ett generellt plan kompletterar dataskyddsförordningen. Vid utförandet av uppdraget är det viktigt att – i den mån utrymme finns på nationell nivå – hitta lämpliga avvägningar mellan skyddet för den personliga integriteten samt myndigheters, företags och enskildas behov av att kunna behandla personuppgifter. Förslagen ska utformas så att företagens administrativa börda inte ökar mer än nödvändigt. En lag som kompletteras av bestämmelser i en förordning samt en viss föreskriftsrätt för tillsynsmyndigheten kan vara en lämplig utgångspunkt för den aktuella kompletterande regleringen.

Utredaren ska därför

- lämna förslag till upphävande av den nuvarande generella personuppgiftsregleringen, och
- lämna förslag till författningsbestämmelser som på ett generellt plan kompletterar dataskyddsförordningen.

I utredarens uppdrag ingår inte att överväga eller lämna förslag till grundlagsändringar. Uppdraget omfattar inte heller att se över eller lämna förslag till förändringar av sådan sektorsspecifik reglering om behandling av personuppgifter som bl.a. finns i de särskilda registerförfattningarna.

Behovet av särskilt författningsstöd för behandling av personuppgifter i den offentliga sektorn

De statliga och kommunala myndigheternas personuppgiftsbehandling kommer huvudsakligen att ske med stöd av de rättsliga grunder som kommer till uttryck i artikel 6.1 c och e i dataskyddsförordningen. Myndigheternas behandling av personuppgifter är alltså i normalfallet antingen nödvändig för att fullgöra en rättslig skyldighet eller utföra en arbetsuppgift av allmänt intresse eller i samband med myndighetsutövning. Detsamma gäller sådan behandling av personuppgifter som sker hos andra än myndigheter vid utförandet av förvaltningsuppgifter, exempelvis bilprovningföretag eller fristående

skolor. Det kan emellertid också gälla för andra verksamheter där arbetsuppgifterna mot bakgrund av verksamhetens syfte bedöms ha ett allmänt intresse.

I dag sker behandling av detta slag till viss del med stöd av reglering i särskilda registerförfattningar men i stor utsträckning enbart med stöd av den generella regleringen i personuppgiftslagen (10 § b), c) och d) PUL). Enligt artikel 6.3 i förordningen måste dock grunden för behandling av personuppgifter som bygger på någon av de rättsliga grunderna i artikel 6.1 c och e fastställas i unionsrätten eller den nationella rätten. Detta innebär att det inte kommer vara möjligt att endast stödja sig på den generella regleringen i förordningen vid sådan behandling. Det behöver därför analyseras vad dataskyddsförordningens krav i denna del innebär i fråga om nationell författningsreglering och om det bör införas generella bestämmelser till stöd för åtminstone den offentliga sektorns behandling av personuppgifter. Informationshanteringsutredningen föreslår en sådan reglering i 8 § i förslaget till myndighetsdatalog (SOU 2015:39). Enligt förslaget får en myndighet behandla personuppgifter om det är nödvändigt för att den ska kunna utföra sin verksamhet. Informationshanteringsutredningens förslag med beaktande av de synpunkter som framförts vid remissbehandlingen är en lämplig utgångspunkt för utredarens analys.

Utredaren ska därför

- analysera om det behövs kompletterande bestämmelser som ger ett generellt stöd för myndigheters och andra organs behandling av personuppgifter, och
- lämna sådana författningsförslag som är behövliga och lämpliga.

Sanktioner

Dataskyddsförordningen innehåller bestämmelser om att tillsynsmyndigheterna ska besluta om administrativa sanktionsavgifter vid överträdelse av förordningens bestämmelser. I artikel 79 finns en detaljerad reglering av vilka faktorer som ska beaktas vid beslut om att utfärda sanktionsavgifter och bestämmande av avgiftens storlek. Kraven på ett effektivt rättsmedel i artikel 79.4 bör för svensk del tillgodoses genom att tillsynsmyndighetens beslut om sanktionsavgifter får överklagas till allmän förvaltningsdomstol.

Enligt artikel 79.3b får varje medlemsstat reglera om och i vilken utsträckning det ska vara möjligt att besluta om sanktionsavgifter mot myndigheter och offentliga organ i den medlemsstaten. Utredaren bör därför analysera om, och i så fall i vilken utsträckning, det bör vara möjligt att besluta om sanktionsavgifter inom den offentliga sektorn. Här bör en jämförelse göras med vad som gäller för t.ex. viten i allmänhet, miljöstraffavgifter och sanktionsavgifter på arbetsmiljöområdet.

Enligt artikel 79b ska medlemsstaterna fastställa regler om sanktioner för överträdelse av förordningen, särskilt för sådana överträdelse som inte är föremål för administrativa sanktionsavgifter. Medlemsstaterna ska också vidta alla åtgärder som är nödvändiga för att säkerställa att dessa bestämmelser tillämpas och underrätta kommissionen om de bestämmelser som antas. Det finns därför behov av att analysera och ta ställning till i vilken utsträckning överträdelse av förordningen bör bli föremål för sådana ytterligare sanktioner i Sverige. Det bör också analyseras om, och i så fall i vilken utsträckning, dessa sanktioner bör vara tillämpliga inom den offentliga sektorn.

I detta sammanhang kan det också behöva analyseras hur en reglering med både administrativa sanktionsavgifter och andra sanktioner förhåller sig till det s.k. dubbelprövningsförbudet i artikel 4.1 i Europakonventionens sjunde tilläggsprotokoll och artikel 50 i EU:s stadga om de grundläggande rättigheterna.

Utredaren ska därför

- analysera vilka kompletterande bestämmelser om administrativa sanktionsavgifter och andra sanktioner som Sverige behöver eller bör införa,
- bedöma om, och i så fall i vilken utsträckning, det bör vara möjligt att besluta om administrativa sanktionsavgifter och andra sanktioner mot myndigheter och offentliga organ,
- analysera om ett system som kan leda till både administrativa sanktionsavgifter och andra sanktioner kan ge upphov till problematik som rör dubbelprövning samt ta ställning till hur detta i så fall bör hanteras, och
- lämna sådana författningsförslag som är behövliga och lämpliga.

Tillsynsmyndigheten

Dataskyddsförordningen föreskriver i likhet med det nuvarande dataskyddsdirektivet att medlemsstaterna ska utse en eller flera självständiga tillsynsmyndigheter som ska ansvara för att övervaka tillämpningen av regleringen. Förordningen innehåller emellertid en betydligt mer detaljerad reglering av tillsynsmyndighetens roll, organisation och uppgifter än vad det nuvarande regelverket gör.

Flertalet av dataskyddsförordningens bestämmelser om tillsynsmyndigheten gäller direkt och medför inga krav på eller behov av kompletterande nationella bestämmelser. Vissa frågor är i och för sig reglerade genom förordningen men tillåter ytterligare nationell reglering. Detta gäller exempelvis regleringen om tillsynsmyndighetens befogenheter i artikel 53. Det är vidare upp till medlemsstaterna att inom vissa angivna ramar reglera bl.a. tillsynsmyndighetens organisation och utnämningen respektive avsättandet av dess medlemmar, samt se till att myndigheten har tillräckliga resurser.

Dataskyddsförordningen innehåller en utförlig reglering som förpliktar de nationella tillsynsmyndigheterna att samarbeta med och assistera andra medlemsstaters tillsynsmyndigheter (artiklarna 54 a och 55). Detta innebär bl.a. skyldigheter att samråda och utbyta information. Tillsynsmyndigheterna ges också möjligheter att genomföra gemensamma insatser och utredningar där personal från olika medlemsstaters tillsynsmyndigheter deltar (artikel 56). Enligt artikel 56.3 får en tillsynsmyndighet, i överensstämmelse med nationell lag, också överföra befogenheter till tillsynsmyndigheter i andra medlemsstater som är involverade i en gemensam insats.

Regeringen beslutade i december 2014 att ge en särskild utredare i uppdrag att utreda om skyddet för den personliga integriteten kan stärkas genom att samla tillsynen över personuppgiftsbehandling hos en myndighet. Utredningen, som antagit namnet Utredningen om tillsynen över den personliga integriteten, ska redovisa sitt uppdrag senast den 30 september 2016. I utredningens uppdrag ingår bl.a. att lämna de förslag som behövs för att myndigheten ska kunna fullgöra de uppgifter som den nu aktuella EU-reformen medför.

Vilken eller vilka myndigheter som ska ha till uppgift att ansvara för tillsynen på dataskyddsförordningens tillämpningsområde (artikel 46.1), anpassningsfrågor som rör myndighetens organisation och

utnämningen respektive avsättandet av medlemmar (artiklarna 47–49 i relevanta delar), nationell representation i Europiska dataskyddsstyrelsen (artikel 46.2) samt resurser (artikel 47.5) och anknytande frågor får anses ligga inom ramen för uppdraget till Utredningen om tillsynen över den personliga integriteten. I den utredningens uppdrag får det också bl.a. anses ingå att överväga om tillsynsmyndigheten bör ges andra befogenheter än de som anges i dataskyddsförordningen (artikel 53.4) samt att analysera vilket utrymme och behov det finns av regler om exempelvis myndighetens uppgifter (artikel 52) i instruktionen till myndigheten. Dessa frågor ingår därför inte i utredarens uppdrag.

I utredarens uppdrag ingår däremot att närmare analysera möjligheten att överföra utredningsbefogenheter till tillsynsmyndigheter i andra medlemsstater.

Utredaren ska därför

- bedöma om det bör införas bestämmelser som möjliggör en överföring av den svenska tillsynsmyndighetens befogenheter till en annan medlemsstats tillsynsmyndighet, och
- lämna lämpliga författningsförslag.

Vissa processuella frågor

Av artikel 53.2 i förordningen framgår att utövandet av tillsynsmyndighetens befogenheter ska vara föremål för lämpliga skyddsåtgärder, bl.a. effektiva rättsmedel. Enligt artikel 53.1 db ska tillsynsmyndigheten ha befogenhet att få tillgång till en personuppgiftsansvarigs eller ett personuppgiftsbiträdes lokaler och utrustning i överensstämmelse med unionsrätten eller nationell processrätt. Vidare anges i artikel 53.3 att varje medlemsstat ska föreskriva att tillsynsmyndigheten ska ha möjlighet att fästa judiciella myndigheters uppmärksamhet på överträdelser av förordningen och, när det är lämpligt, inleda eller på annat sätt delta i rättsliga processer för att se till att förordningen efterlevs.

Den registrerade ska, enligt dataskyddsförordningen, ha en rätt att framföra klagomål hos tillsynsmyndigheten (artikel 73.1). Vidare ska fysiska och juridiska personer ha en rätt till ett effektivt rättsmedel mot tillsynsmyndighetens rättsligt bindande beslut som rör dem (artikel 74.1). Detta torde för svensk del bäst tillgodoses ge-

nom en rätt för enskilda att överklaga tillsynsmyndighetens beslut till allmän förvaltningsdomstol.

Enligt artikel 74.2 ska registrerade som framfört ett klagomål till tillsynsmyndigheten ha en rätt till ett effektivt rättsmedel om myndigheten inte hanterar klagomålet eller informerar den registrerade om utgången inom tre månader. Detta torde innebära att den registrerade under vissa förhållanden ska ha möjlighet att föra en dröjsmålstalan mot tillsynsmyndigheten.

En registrerad ska vidare ha en rätt till ett effektivt rättsmedel direkt mot en personuppgiftsansvarig eller ett personuppgiftsbiträde om den registrerade anser sig ha fått sina rättigheter enligt förordningen åsidosatta (artikel 75). I enlighet med artikel 76.1 i dataskyddsförordningen ska den registrerade också ha rätt att ge mandat till en integritetsskyddsorganisation att företräda honom eller henne gentemot tillsynsmyndigheten och processa i domstol. Det bör för svenskt vidkommande inte vara aktuellt att utnyttja möjligheten enligt förordningen att ge en sådan organisation rätt att föra talan även utan den registrerades mandat (artikel 76.2).

Om en behörig nationell domstol har information om att en process som rör samma sak redan pågår i en domstol i en annan medlemsstat får domstolen under vissa förutsättningar vilandeförklara målet (artikel 76a.1 och 76a.2). En domstol i första instans kan också efter ansökan av någon av parterna förklara sig sakna behörighet om den andra medlemsstatens domstol har behörighet och lagen i den medlemsstaten tillåter en förening av målen (artikel 76a.2a).

I dataskyddsförordningen finns vidare bestämmelser om skadestånd (artikel 77). En enskild som har drabbats av materiell eller immateriell skada genom att hans eller hennes personuppgifter har behandlats på ett sätt som inte är förenligt med förordningen har under vissa närmare angivna förutsättningar rätt till ersättning av den personuppgiftsansvarige eller dennes personuppgiftsbiträde. Förordningen reglerar i vilken medlemsstat en talan om skadestånd ska väckas medan nationell rätt styr vilken domstol i den medlemsstaten som är behörig (artikel 75.2 och artikel 77.6).

Behovet av kompletterande nationella bestämmelser i de ovanstående frågorna behöver bli föremål för närmare analys.

Utredaren ska därför

- analysera i vilken utsträckning det behövs kompletterande bestämmelser om utövandet av tillsynsmyndighetens befogenheter,
- analysera i vilken utsträckning det behövs kompletterande bestämmelser om de rättsmedel för enskilda som regleras i dataskyddsförordningen,
- analysera om det behövs kompletterande bestämmelser om sådana integritetsskyddsorganisationer som regleras i förordningen,
- analysera om det behövs kompletterande bestämmelser om vilandeförklaring eller skadestånd, och
- lämna sådana författningsförslag som är behövliga och lämpliga.

Sekretessfrågor

Enligt 32 kap. 1 § offentlighets- och sekretesslagen (2009:400), förkortad OSL, gäller sekretess hos Datainspektionen, bl.a. i ärenden om tillstånd eller tillsyn som enligt lag eller annan författning ska handläggas av inspektionen. Sekretessen gäller för uppgifter om en enskilds personliga eller ekonomiska förhållanden, om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs. I 11 kap. 1 § första stycket OSL finns dessutom vissa bestämmelser om överföring av sekretess i tillsynsverksamhet.

I förarbetena till personuppgiftslagen framhålls att motsvarigheten till 32 kap. 1 § OSL i den nu upphävda sekretesslagen (1980:100) vid behov skulle tolkas EG-konformt i förhållande till kravet på tystnadsplikt för tillsynsmyndighetens medlemmar och personal i dataskyddsdirektivets artikel 28.7 (propositionen Personuppgiftslag, prop. 1997/98:44 s. 146). I artikel 49.2 i dataskyddsförordningen finns ett motsvarande krav på tystnadsplikt och det behöver analyseras om denna artikel innebär behov av att anpassa de nuvarande sekretessbestämmelserna på något sätt.

Enligt artikel 36.4 ska ett uppgiftsskyddsombud vara bundet av sekretess eller tystnadsplikt rörande utförandet av hans eller hennes uppgifter i enlighet med unionsrätten eller nationell rätt. Någon motsvarande reglering finns inte i det nuvarande dataskyddsdirek-

tivet. Det behöver utredas vilken reglering som behöver införas i svensk rätt med anledning av denna artikel.

Enligt 21 kap. 7 § OSL gäller sekretess för personuppgift om det kan antas att ett utlämnande skulle medföra att uppgiften behandlas i strid med personuppgiftslagen. Eftersom personuppgiftslagen ska upphävas behöver bestämmelsen ses över. Även 10 kap. 27 § och 40 kap. 5 § OSL innehåller hänvisningar till personuppgiftslagen och behöver anpassas till den nya regleringen.

Utredaren ska därför

- analysera om nuvarande sekretessbestämmelser behöver anpassas med anledning av förordningens reglering om tystnadsplikt hos tillsynsmyndigheten,
- analysera vilken reglering som behöver införas i svensk rätt med anledning av förordningens bestämmelser om sekretess och tystnadsplikt för personuppgiftsombud,
- överväga hur de bestämmelser i offentlighets- och sekretesslagen som innehåller hänvisningar till personuppgiftslagen bör anpassas till den nya regleringen, och
- lämna sådana författningsförslag som är behövliga och lämpliga.

Nationella begränsningar av vissa skyldigheter och rättigheter

Genom artikel 21.1 i dataskyddsförordningen ges medlemsstaterna möjlighet att begränsa omfattningen av vissa av de skyldigheter och rättigheter som förordningen föreskriver. Detta gäller bl.a. informationsskyldigheten (artiklarna 14–15) och rätten för den registrerade att motsätta sig behandling (artikel 19). Sådana begränsningar får göras endast om de är förenliga med det väsentliga innehållet i de grundläggande fri- och rättigheterna samt är en nödvändig och proportionerlig åtgärd i ett demokratiskt samhälle till skydd för vissa angivna intressen, såsom nationell säkerhet, försvaret, allmän säkerhet eller förebyggande, undersökning eller avslöjande av brott. I artikel 21.2 finns vidare krav på vad nationella bestämmelser med denna typ av begränsningar ska innehålla.

I det nuvarande dataskyddsdirektivet finns motsvarande reglering om undantag i artikel 13. Undantag med stöd av den bestämmelsen tas ofta in i sektorsspecifik lagstiftning. I 8 a § PUL finns

emellertid ett generellt bemyndigande för regeringen att meddela föreskrifter om undantag av detta slag. I förarbetena till paragrafen uttalas att det kan uppkomma situationer som inte har varit möjliga att förutse vid utarbetandet av särlagstiftning och att det därför är befogat att regeringen har möjlighet att föreskriva om undantag, t.ex. i avvaktan på att särlagstiftning hinner utarbetas eller ändras (propositionen Översyn av personuppgiftslagen, prop. 2005/06:173 s. 56). I 27 § PUL finns vidare ett särskilt undantag till informationsskyldigheten vid sekretess och tystnadsplikt. I utredningens uppdrag bör ingå att överväga om det finns behov av bestämmelser av detta slag i den generella regleringen som ska komplettera förordningen.

Utredaren ska därför

- överväga om det bör införas bestämmelser om undantag till vissa av förordningens skyldigheter och rättigheter i den kompletterande regleringen, och
- lämna lämpliga författningsförslag.

Kompletterande regler om behandling av känsliga personuppgifter och uppgifter om lagöverträdelser

Dataskyddsförordningen innehåller i likhet med dataskyddsdirektivet och personuppgiftslagen ett principiellt förbud mot att behandla känsliga personuppgifter (artikel 9.1). Med känsliga personuppgifter avses uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetiska uppgifter, biometriska uppgifter som specifikt behandlas för att unikt identifiera individer eller uppgifter som rör hälsa eller sexualliv. Förbudet är förenat med ett antal viktiga undantag (artikel 9.2–9.5). För att vissa av undantagen ska vara tillämpliga krävs att grunden för sådana behandlingar på olika sätt kommer till uttryck i unionsrätten eller i nationell lagstiftning.

Möjligheten att göra undantag från förbudet kommer i svensk rätt i stor utsträckning att utnyttjas genom sektorsspecifik lagstiftning. I dag finns dock vissa undantagsbestämmelser i 15–19 §§ PUL. Som exempel kan nämnas att känsliga personuppgifter, enligt 19 § andra stycket PUL, får behandlas för forskningsändamål om

behandlingen godkänts enligt lagen (2003:460) om etikprövning av forskning som avser människor.

Det finns i dag också en möjlighet för regeringen eller den myndighet som regeringen bestämmer att enligt 20 § PUL meddela föreskrifter om ytterligare undantag om det behövs med hänsyn till ett viktigt allmänt intresse. Med stöd av detta bemyndigande har regeringen föreskrivit att myndigheter får behandla känsliga personuppgifter i löpande text om uppgifterna har lämnats in i ett ärende eller är nödvändiga för handläggningen av det (8 § PUF).

Utgångspunkten bör vara att det även i fortsättningen kommer att behövas vissa bestämmelser om undantag från förbudet att behandla känsliga personuppgifter av det slag som i dag finns i personuppgiftslagen och personuppgiftsförordningen. Det bör därför ingå i uppdraget att analysera hur sådana bestämmelser kan utformas i den kompletterande regleringen.

Behandling av personuppgifter om lagöverträdelse och liknande uppgifter som i dag regleras i 21 § PUL kommer genom artikel 9a i dataskyddsförordningen även fortsättningsvis att vara föremål för särskilda begränsningar. Som huvudregel får sådana uppgifter endast behandlas under kontroll av en officiell myndighet eller om det är tillåtet i unionsrätten eller i nationell rätt, som i så fall ska innehålla adekvata regler till skydd för den registrerades fri- och rättigheter.

I likhet med vad som gäller för känsliga personuppgifter får personuppgifter om lagöverträdelse och liknande uppgifter, enligt 21 § andra stycket PUL, behandlas för forskningsändamål om behandlingen har godkänts enligt lagen om etikprövning av forskning som avser människor. Även här har regeringen eller den myndighet regeringen bestämmer möjlighet att meddela föreskrifter om ytterligare undantag. Till detta kommer en möjlighet för regeringen att besluta om undantag i enskilda fall, som också kan överlätas åt tillsynsmyndigheten.

I uppdraget bör ingå att analysera i vilken utsträckning det bör införas regler i den kompletterande regleringen som tillåter behandling av uppgifter om lagöverträdelse som inte sker under kontroll av en officiell myndighet. En lämplig utgångspunkt för en sådan analys är den befintliga regleringen om behandling för forskningsändamål och den delegerade föreskriftsrätten i personuppgiftslagen.

Utredaren ska därför

- överväga vilka kompletterande bestämmelser om undantag från förbudet att behandla känsliga personuppgifter som bör finnas i den generella regleringen,
- analysera i vilken utsträckning det bör införas regler i den kompletterande regleringen som tillåter behandling av uppgifter om lagöverträdelser som inte sker under kontroll av en officiell myndighet, och
- lämna lämpliga författningsförslag.

Kompletterande regler om behandling av personnummer eller samordningsnummer

I 22 § PUL finns särskilda bestämmelser om när personnummer eller samordningsnummer får behandlas. Bestämmelsen är ett genomförande av artikel 8.7 i dataskyddsdirektivet där det föreskrivs att medlemsstaterna ska bestämma på vilka villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas.

Även dataskyddsförordningen ger medlemsstaterna möjlighet att bestämma särskilda villkor för när ett nationellt identifieringsnummer eller liknande identifieringsuppgift får behandlas (artikel 80b). Enligt förordningen ska sådana villkor innebära att identifieringsuppgifterna bara får användas om det vidtas lämpliga åtgärder till skydd för den registrerades fri- och rättigheter i enlighet med förordningen. I uppdraget bör det ingå att överväga om det även fortsättningsvis bör finnas begränsande villkor för behandling av personnummer eller samordningsnummer.

Utredaren ska därför

- överväga om särskilda villkor bör gälla för behandling av personnummer eller samordningsnummer, och
- lämna lämpliga författningsförslag.

Krav på förhandstillstånd för vissa särskilt integritetskänsliga behandlingar?

Enligt dataskyddsförordningen krävs att den personuppgiftsansvarige gör en dataskyddskonsekvensanalys före vissa typer av högrisk-behandlingar av personuppgifter (artikel 33). Om en sådan konsekvensanalys indikerar att den tänkta behandlingen skulle innebära en hög risk, ska den personuppgiftsansvarige under vissa förutsättningar och på ett visst sätt samråda med tillsynsmyndigheten (artikel 34.2–34.6). Enligt artikel 34.7a har medlemsstaterna dessutom möjlighet att införa krav på förhandstillstånd för sådana behandlingar som utförs i det allmännas intresse, inklusive behandling av uppgifter som rör socialt skydd och folkhälsa.

Enligt 41 § PUL har regeringen i dag möjlighet att meddela föreskrifter om att behandlingar som innebär särskilda risker för otillbörligt intrång i den personliga integriteten ska anmälas för förhandskontroll till tillsynsmyndigheten. Det har tidigare funnits vissa sådana bestämmelser i personuppgiftsförordningen men dessa har upphävts. Viss behandling som regleras i särskild ordning, t.ex. Skatteverkets behandling av personuppgifter i samband med brottsutredningar, omfattas däremot av bestämmelser om förhandskontroll. I sammanhanget kan också huvudregeln i kameraövervakningslagen (2013:460) nämnas som innebär att det krävs tillstånd från länsstyrelsen för att en övervakningskamera ska få vara uppsatt så att den kan riktas mot en plats dit allmänheten har tillträde.

Det bör mot denna bakgrund övervägas om regeringen också fortsättningsvis ska ha en generell möjlighet att meddela föreskrifter i frågan om krav på förhandstillstånd eller om sådana föreskrifter endast bör tas in i sådan sektorsspecifik lagstiftning som ligger utanför utredningens uppdrag.

Utredaren ska därför

- överväga om regeringen även fortsättningsvis ska ges en generell rätt att meddela föreskrifter om krav på förhandstillstånd i vissa fall, och
- lämna lämpliga författningsförslag.

Barns samtycke i vissa fall

Enligt artikel 6.1 a i dataskyddsförordningen kan den registrerades samtycke utgöra en rättslig grund för behandling av personuppgifter. För att ett samtycke ska vara giltigt när informationssamhällets tjänster erbjuds direkt till ett barn under 16 år krävs, enligt artikel 8.1 i förordningen, vårdnadshavarens samtycke eller dennes godkännande av barnets samtycke. Den personuppgiftsansvarige ska i dessa fall göra rimliga ansträngningar för att kontrollera att samtycke ges eller godkänns av vårdnadshavaren. Medlemsstaterna har möjlighet att sänka den aktuella åldersgränsen från 16 år till lägst 13 år, vilket motsvarar den åldersgräns som vissa tjänsteleverantörer använder sig av. De aktuella bestämmelserna i förordningen ska inte påverka den allmänna kontraktsrätten i medlemsstaterna, såsom regler om giltighet, ingående eller verkan av ett avtal med ett barn (artikel 8.2).

I personuppgiftslagen saknas motsvarande särbestämmelser för barns samtycke. En bedömning av om den underåriges samtycke ska anses giltigt får som huvudregel därmed göras från fall till fall. För ett giltigt samtycke krävs att den registrerade är kapabel att förstå innebörden av samtycket. Enligt Datainspektionen kan en tumregel vara att den som är 15 år normalt anses kapabel att ta ställning i samtyckesfrågan. Det kan dock finnas andra rättsliga hinder mot vissa typer av personuppgiftsbehandlingar, exempelvis när det gäller att skicka direktreklam till barn.

Utredaren ska mot denna bakgrund

- analysera för- och nackdelar med att sätta en lägre åldersgräns än förordningens 16 år när det gäller krav på vårdnadshavares samtycke eller dennes godkännande av barnets samtycke, och
- lämna lämpliga författningsförslag.

Hur ska certifieringsorgan godkännas?

Dataskyddsförordningen innehåller liksom nuvarande reglering bestämmelser om att bl.a. medlemsstaterna och tillsynsmyndigheterna ska uppmuntra till att sammanslutningar av personuppgiftsansvariga tar fram uppförandekoder för personuppgiftsbehandlingen i en viss bransch eller liknande (artikel 38). Syftet är att bidra till en korrekt tillämpning av förordningen. Utkast till uppförandekoder ska

kunna ges in till tillsynsmyndigheten för att därefter godkännas och publiceras enligt en viss procedur. Tillsynsmyndigheterna har också möjlighet att godkänna särskilda organ som, vid sidan av tillsynsmyndigheten, ska övervaka att de godkända uppförandekoderna följs (artikel 38a).

Enligt artikel 39 i dataskyddsförordningen ska medlemsstaterna, Europiska dataskyddsstyrelsen och kommissionen, framför allt på unionsnivå, även uppmuntra till att det införs certifieringsmekanismer och märkningar i syfte att personuppgiftsansvariga och personuppgiftsbiträden ska kunna visa att de uppfyller kraven i förordningen. Sådan certifiering kan antingen utföras av särskilda certifieringsorgan eller av tillsynsmyndigheten. Dataskyddsförordningen kräver att medlemsstaterna inför bestämmelser för hur sådana särskilda certifieringsorgan ska godkännas (artikel 39a). Ett sådant organ kan antingen godkännas av tillsynsmyndigheten eller genom ackreditering enligt Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter.

Utredaren ska därför

- bedöma hur certifieringsorgan ska godkännas, och
- lämna sådana författningsförslag som är behövliga och lämpliga.

Förhållandet till yttrande- och informationsfriheten och offentlighetsprincipen

Enligt beaktandesats 72 i det nuvarande dataskyddsdirektivet är det möjligt att vid genomförandet av direktivet ta hänsyn till principen om allmänhetens rätt till tillgång till allmänna handlingar. Vidare ska medlemsstaterna, enligt artikel 9 i direktivet, med avseende på behandling av personuppgifter som sker uteslutande för journalistiska ändamål eller konstnärligt eller litterärt skapande, besluta om undantag och avvikelser från delar av direktivet om det är nödvändigt för att förena rätten till privatlivet med reglerna om yttrandefriheten.

Vid genomförandet av dataskyddsdirektivet gjorde regeringen bedömningen att tryckfrihetsförordningen och yttrandefrihetsgrundlagen inte behövde ändras (prop. 1997/98:44 s. 50). I 7 § första stycket PUL finns en upplysningsbestämmelse om att bestämmelserna i lagen inte ska tillämpas i den utsträckning det skulle strida mot

bestämmelserna i tryckfrihetsförordningen och yttrandefrihetsgrundlagen. I 8 § första stycket PUL upplyses vidare att bestämmelserna i lagen inte tillämpas i den utsträckning det skulle inskränka en myndighets skyldighet enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter. När det gäller förhållandet till yttrande- och informationsfriheten utanför tryckfrihetsförordningens och yttrandefrihetsgrundlagens tillämpningsområde görs i 7 § andra stycket PUL undantag från flertalet av lagens bestämmelser vid personuppgiftsbehandling som sker uteslutande för journalistiska ändamål eller konstnärligt eller litterärt skapande. Undantaget för journalistiska ändamål är inte begränsat till journalister eller traditionella massmedier. Även en privatperson kan anses behandla personuppgifter för sådana ändamål, t.ex. på en blogg.

I dataskyddsförordningen finns bestämmelser som ger ett tydligt utrymme för nationell reglering om förhållandet mellan, å ena sidan, skyddet för personuppgifter och, å andra sidan, yttrande- och informationsfriheten och offentlighetsprincipen.

Enligt artikel 80.1 i dataskyddsförordningen ska medlemsstaternas nationella lagstiftning förena rätten till skydd av personuppgifter i enlighet med förordningen med rätten till yttrande- och informationsfrihet. Detta ska omfatta personuppgiftsbehandling för journalistiska och akademiska ändamål samt för konstnärligt eller litterärt skapande. När det gäller behandling för sådana ändamål ska medlemsstaterna enligt artikel 80.2 föreskriva om undantag eller avvikelser från stora delar av förordningens bestämmelser om det behövs för att förena rätten till skydd för personuppgifter med yttrande- och informationsfriheten. Medlemsstaterna ska enligt artikel 80.3 underrätta kommissionen om de undantagsbestämmelser som de har antagit med stöd av denna reglering.

Enligt artikel 80a i dataskyddsförordningen får personuppgifter i allmänna handlingar hos en myndighet eller vissa typer av organ lämnas ut i enlighet med unionsrätten eller nationell rätt i syfte att förena allmänhetens tillgång till allmänna handlingar med rätten till skydd av personuppgifter i enlighet med förordningen.

Enligt regeringens bedömning innebär denna reglering att det blir tydligare än i det nuvarande dataskyddsdirektivet att den EU-rättsliga dataskyddsregleringen inte inkräktar på området för tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Som konstateras under avsnittet om de allmänna riktlinjerna för uppdraget ingår det därför

inte i utredarens uppdrag att överväga eller lämna förslag till grundlagsändringar.

Utanför tryckfrihetsförordningens och yttrandefrihetsgrundlagens tillämpningsområde torde det även fortsättningsvis finnas behov av bestämmelser som – liksom 7 § andra stycket PUL – balanserar personuppgiftsskyddet mot yttrande- och informationsfriheten. Det bör därför ingå i uppdraget att analysera hur sådana regler bör utformas.

Utredaren ska därför

- analysera hur bestämmelser som balanserar personuppgiftsskyddet mot yttrande- och informationsfriheten utanför tryckfrihetsförordningens och yttrandefrihetsgrundlagens tillämpningsområde bör utformas, och
- lämna sådana författningsförslag som är behövliga och lämpliga.

Myndigheters bevarande av allmänna handlingar och behandling av personuppgifter för arkivering i allmänhetens intresse samt för vetenskapliga eller historiska forskningsändamål eller för statistiska ändamål

I personuppgiftslagen finns vissa centrala bestämmelser som rör lagens förhållande till myndigheters arkivering av allmänna handlingar och sådan personuppgiftsbehandling som sker för historiska, statistiska eller vetenskapliga ändamål.

Av 8 § andra stycket PUL framgår att lagens bestämmelser inte hindrar att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. I förarbetena till personuppgiftslagen bedömdes att myndigheternas bevarande av allmänna handlingar är tillåtet enligt de grundläggande bestämmelserna i dataskyddsdirektivet, så länge de inte innehåller känsliga personuppgifter. Det bedömdes däremot att ett särskilt undantag krävdes för att myndigheterna också skulle kunna bevara känsliga personuppgifter. Det aktuella undantaget i 8 § andra stycket PUL omfattar också den insamling och det långtidsbevarande av personuppgifter som sker hos de särskilda arkivmyndigheterna (prop. 1997/98:44 s. 47–48).

I 9 § PUL – där de grundläggande kraven på behandlingen av personuppgifter regleras – finns vissa bestämmelser som särskilt rör behandling för historiska, statistiska eller vetenskapliga ändamål. Här

framgår exempelvis att en behandling av personuppgifter för sådana ändamål inte ska anses oförenlig med insamlingsändamålen (andra stycket). Det finns vidare regler om hur länge personuppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål (tredje stycket) och begränsningar av när personuppgifter som behandlas för sådana ändamål får användas för att vidta åtgärder i fråga om den registrerade (fjärde stycket). Begränsningen i 9 § fjärde stycket PUL är en sådan lämplig skyddsåtgärd som krävs enligt artikel 6 i dataskyddsdirektivet. Enligt 8 § andra stycket PUL gäller dock inte denna begränsning för myndigheters användning av personuppgifter i allmänna handlingar. Detta undantag bygger på att det för sådana personuppgifter finns andra lämpliga skyddsåtgärder i form av bestämmelser om sekretess och skydd för arkiv (prop. 1997/98:44 s. 64).

I dataskyddsförordningen finns ett antal bestämmelser som särskilt rör personuppgiftsbehandling för arkivändamål i allmänhetens intresse samt för vetenskapliga eller historiska forskningsändamål eller för statistiska ändamål. Enligt artikel

5.1 b gäller exempelvis att behandling av personuppgifter för sådana ändamål, i enlighet med artikel 83.1, inte ska anses oförenlig med de ursprungliga ändamålen. Av artikel 5.1 e följer att personuppgifter får lagras under en längre tid än vad som normalt gäller, om uppgifterna enbart kommer att behandlas för arkivändamål i allmänhetens intresse eller för vetenskapliga eller historiska forskningsändamål eller för statistiska ändamål. Den förlängda bevarandetiden gäller i den mån som lämpliga tekniska och organisatoriska åtgärder vidtas i enlighet med kraven i artikel 83.1 för att skydda de registrerades fri- och rättigheter. Det finns också särskilda bestämmelser som innebär undantag från förbudet att behandla känsliga personuppgifter för aktuella ändamål i artikel 9.2 i, vilket har berörts i ett tidigare avsnitt.

I artikel 19.2aa i dataskyddsförordningen föreskrivs vidare att den registrerade ska ha rätt att motsätta sig behandling för vetenskapliga eller historiska forskningsändamål eller för statistiska ändamål av skäl som rör hans eller hennes personliga situation, om inte behandlingen är nödvändig för utförandet av en arbetsuppgift av allmänt intresse. Genom artikel 83.2 och 83.3 ges medlemsstaterna möjlighet att föreskriva om undantag från denna och vissa andra av rättigheterna i förordningen. Detta får emellertid bara göras i den mån det kan antas att de aktuella rättigheterna skulle göra det omöjligt eller allvarligt försvå-

ra uppnåendet av de särskilda ändamålen med behandlingen och sådana undantag är nödvändiga för att ändamålen ska kunna uppfyllas.

De generella kraven på skyddsåtgärder i artikel 83.1 och särskilda bestämmelser om exempelvis lagringstid och gallring aktualiseras i stor utsträckning i sektorsspecifik lagstiftning. Detsamma gäller behovet av undantag med stöd av artikel 83.2 och 82.3 i förordningen. Det är emellertid av central betydelse att myndigheternas bevarande av allmänna handlingar inte hindras av dataskyddsregleringen och att myndigheternas möjlighet att använda uppgifter i dessa handlingar säkerställs. På samma sätt behöver en ändamålsenlig behandling av personuppgifter för annan arkivering i allmänhetens intresse samt för vetenskapliga eller historiska forskningsändamål eller för statistiska ändamål garanteras, samtidigt som skyddet för den registrerades fri- och rättigheter beaktas. Utgångspunkten bör därför vara att vissa grundläggande bestämmelser, liknande de som i dag finns i personuppgiftslagen, behöver tas in i den generella regleringen som ska komplettera dataskyddsförordningen.

Utredaren ska därför

- analysera vilka kompletterande bestämmelser om myndigheters bevarande av allmänna handlingar, användning av uppgifter i dessa och överlämnande av arkivmaterial till en arkivmyndighet som behövs i den generella regleringen,
- analysera vilka övriga kompletterande bestämmelser om behandling av personuppgifter för arkivering i allmänhetens intresse samt för vetenskapliga eller historiska forskningsändamål eller för statistiska ändamål som bör finnas i den generella regleringen, och
- lämna lämpliga författningsförslag.

Personuppgiftsbehandling utanför EU-rättens tillämpningsområde

Personuppgiftslagen är generellt tillämplig vilket innebär att den också gäller för sådan behandling som faller utanför det nuvarande dataskyddsdirektivets tillämpningsområde, t.ex. statens verksamhet på straffrättens område, allmän säkerhet och försvar. Anledningen till att man valde denna lösning var bl.a. att det ansågs särskilt viktigt med ett starkt integritetsskydd för personuppgifter inom all offentlig verksamhet. Vidare ansågs den valda lösningen garantera

att behovet av särregler i förhållande till personuppgiftslagen alltid övervägs noga i den ordning som krävs för författningsgivning (prop. 1997/98:44 s. 40–41).

Dataskyddsförordningens tillämpningsområde motsvarar huvudsakligen det nuvarande dataskyddsdirektivets. Det nya dataskyddsdirektivets tillämpningsområde omfattar dock – till skillnad från det nuvarande dataskyddsrambeslutet – myndigheters rent nationella personuppgiftsbehandling för brottsbekämpande och liknande ändamål. Detta innebär att den nya EU-rättsliga dataskyddsregleringen kommer att täcka ett något större område. Det kommer emellertid fortfarande att finnas ett område som inte täcks av EU-regleringen.

Inom detta område har Sverige i dag vissa särskilda regelverk för behandling av personuppgifter, t.ex. lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet. Av 1 § andra stycket i respektive lag framgår att personuppgiftslagen inte gäller vid personuppgiftsbehandling enligt den aktuella lagen. För Försvarsmaktens och Försvarets radioanstalts övriga verksamheter där personuppgiftsbehandling kan förekomma, t.ex. i samband med myndigheternas interna och administrativa åtgärder, tillämpas till största del personuppgiftslagen.

Lagen (1998:938) om behandling av personuppgifter om totalförsvarspliktiga är ett exempel på lagstiftning som gäller utöver personuppgiftslagen. Det innebär att personuppgiftslagens regler är tillämpliga i den utsträckning det inte finns avvikande bestämmelser i lagen om behandling av personuppgifter om totalförsvarspliktiga.

I utredarens uppdrag ingår inte att se över de lagar på försvarsområdet som nu har nämnts eller andra sektorsspecifika särregleringar. Det kan emellertid förekomma personuppgiftsbehandling utanför EU-rättens tillämpningsområde som inte omfattas av någon sektorspecifik reglering. Utredaren bör undersöka denna fråga närmare och överväga om det finns behov av en generell reglering för sådan personuppgiftsbehandling. En sådan reglering skulle exempelvis kunna innebära att bestämmelserna i förordningen i relevanta delar görs tillämpliga inom detta område.

Utredaren ska därför

- undersöka om det finns personuppgiftsbehandling utanför EU-rättens tillämpningsområde som inte omfattas av särreglering,

- överväga om det behöver införas generella bestämmelser för sådan personuppgiftsbehandling, och
- lämna sådana författningsförslag som är behövliga och lämpliga.

Förhållandet till sektorsspecifik reglering och behovet av övergångsbestämmelser

Personuppgiftslagen är subsidiär, vilket innebär att lagen inte ska tillämpas om det finns avvikande bestämmelser i en annan lag eller förordning (2 § PUL). Sådana bestämmelser finns bl.a. i särskilda registerförfattningar. Frågan om förhållandet till sektorsspecifik reglering kan aktualiseras även när det gäller den kompletterande reglering som utredaren ska lägga fram förslag till. Så kan exempelvis vara fallet när det gäller eventuella förslag till bestämmelser om stöd för behandling av personuppgifter i den offentliga sektorn och till generell reglering för personuppgiftsbehandling utanför EU-rättens tillämpningsområde. I uppdraget ingår därför att analysera om det finns behov att reglera förhållandet mellan den kompletterande regleringen och sektorspecifika föreskrifter.

Personuppgiftslagen måste upphävas redan i samband med att dataskyddsförordningen börjar tillämpas. Det kan därför finnas behov av övergångsbestämmelser som i första hand innebär att lagen under en övergångsperiod fortsätter att gälla för sådan personuppgiftsbehandling som inte täcks av förordningens tillämpningsområde.

Utredaren ska därför

- analysera hur bestämmelserna i det kompletterande generella regelverket bör förhålla sig till bestämmelser om behandling av personuppgifter i annan lag eller förordning,
- lämna behövliga och lämpliga författningsförslag, och
- lämna förslag till lämpliga övergångsbestämmelser.

Övriga frågor

Utredaren är oförhindrad att inom de ramar som anges i de allmänna riktlinjerna ta upp och belysa även andra frågeställningar som är relevanta för uppdraget. Om utredaren kommer fram till att det krävs

eller är lämpligt med kompletterande generella nationella bestämmelser i andra delar än de som ska utredas särskilt, ska sådana föreslås.

Konsekvensbeskrivningar

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för det allmänna och för enskilda. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras. Utredaren ska särskilt ange konsekvenser för företagen i form av kostnader och ökade administrativa bördor. Utredaren ska också redovisa förslagets konsekvenser för den personliga integriteten.

Samråd och redovisning av uppdraget

Utredaren ska hålla sig informerad om och beakta relevant arbete som bedrivs inom Regeringskansliet, utredningsväsendet och inom EU. Vid anpassningen av svensk rätt till den nya EU-regleringen bör en enhetlig tolkning av regelverket eftersträvas. Utredaren ska därför följa och i lämplig omfattning samråda med övriga utredningar som har i uppdrag att anpassa svensk rätt till reformen av EU:s dataskyddsregelverk. Till sådana utredningar hör bl.a. utredningen om tillsynen över den personliga integriteten (Ju 2015:02) och utredningen om kameraövervakningslagen – brottsbekämpning och integritetsskydd (Ju 2015:14), samt den kommande utredningen om genomförandet av det nya dataskyddsdirektivet. Samråd är särskilt viktigt i processuella frågor och frågor som rör sanktioner, tillsynsmyndigheten och arkivering. Under genomförandet av uppdraget ska utredaren, i den utsträckning som bedöms lämplig, också ha en dialog med och inhämta upplysningar från myndigheter, näringslivet och andra som kan vara berörda av aktuella frågor.

Uppdraget ska redovisas senast den 12 maj 2017.

(Justitiedepartementet)

I

(Lagstiftningsakter)

FÖRORDNINGAR

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679

av den 27 april 2016

om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 16,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ⁽¹⁾,

med beaktande av Regionkommitténs yttrande ⁽²⁾,

i enlighet med det ordinarie lagstiftningsförfarandet ⁽³⁾, och

av följande skäl:

- (1) Skyddet för fysiska personer vid behandling av personuppgifter är en grundläggande rättighet. Artikel 8.1 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*) och artikel 16.1 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) föreskriver att var och en har rätt till skydd av de personuppgifter som rör honom eller henne.
- (2) Principerna och reglerna för skyddet för fysiska personer vid behandling av deras personuppgifter bör, oavsett deras medborgarskap eller hemvist, respektera deras grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Avsikten med denna förordning är att bidra till att skapa ett område med frihet, säkerhet och rättvisa och en ekonomisk union, till ekonomiska och sociala framsteg, till förstärkning och konvergens av ekonomierna inom den inre marknaden samt till fysiska personers välbefinnande.
- (3) Europaparlamentets och rådets direktiv 95/46/EG ⁽⁴⁾ syftar till att harmonisera skyddet av fysiska personers grundläggande rättigheter och friheter vid behandling av personuppgifter och att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna.

⁽¹⁾ EUT C 229, 31.7.2012, s. 90.

⁽²⁾ EUT C 391, 18.12.2012, s. 127.

⁽³⁾ Europaparlamentets ståndpunkt av den 12 mars 2014 (ännu ej offentliggjord i EUT) och rådets ståndpunkt vid första behandlingen av den 8 april 2016 (ännu ej offentliggjord i EUT). Europaparlamentets ståndpunkt av den 14 april 2016.

⁽⁴⁾ Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGTL 281, 23.11.1995, s. 31).

- (4) Behandlingen av personuppgifter bör utformas så att den tjänar människor. Rätten till skydd av personuppgifter är inte en absolut rättighet; den måste förstås utifrån sin uppgift i samhället och vägas mot andra grundläggande rättigheter i enlighet med proportionalitetsprincipen. Denna förordning respekterar alla grundläggande rättigheter och iakttar de friheter och principer som erkänns i stadgan, såsom de fastställda i fördragen, särskilt skydd för privat- och familjeliv, bostad och kommunikationer, skydd av personuppgifter, tankefrihet, samvetsfrihet och religionsfrihet, yttrande- och informationsfrihet, näringsfrihet, rätten till ett effektivt rättsmedel och en opartisk domstol samt kulturell, religiös och språklig mångfald.
- (5) Den ekonomiska och sociala integration som uppstått tack vare den inre marknaden har lett till en betydande ökning av de gränsöverskridande flödena av personuppgifter. Utbytet av personuppgifter mellan offentliga och privata aktörer, inbegripet fysiska personer, sammanslutningar och företag, över hela unionen har ökat. Nationella myndigheter i medlemsstaterna uppmanas i unionsrätten att samarbeta och utbyta personuppgifter för att vara i stånd att fullgöra sina uppdrag eller utföra arbetsuppgifter för en myndighet som finns i en annan medlemsstat.
- (6) Den snabba tekniska utvecklingen och globaliseringen har skapat nya utmaningar vad gäller skyddet av personuppgifter. Omfattningen av insamling och delning av personuppgifter har ökat avsevärt. Tekniken gör det möjligt för både privata företag och offentliga myndigheter att i sitt arbete använda sig av personuppgifter i en helt ny omfattning. Allt fler fysiska personer gör sina personliga uppgifter allmänt tillgängliga, världen över. Tekniken har omvandlat både ekonomin och det sociala livet, och bör ytterligare underlätta det fria flödet av personuppgifter inom unionen samt överföringar till tredjeländer och internationella organisationer, samtidigt som en hög skyddsnivå säkerställs för personuppgifter.
- (7) Dessa förändringar kräver en stark och mer sammanhängande ram för dataskyddet inom unionen, uppbackad av kraftfullt tillsynsarbete, eftersom det är viktigt att skapa den tillit som behövs för att utveckla den digitala ekonomin över hela den inre marknaden. Fysiska personer bör ha kontroll över sina egna personuppgifter. Den rättsliga säkerheten och smidigheten för fysiska personer, ekonomiska operatörer och myndigheter bör stärkas.
- (8) Om denna förordning föreskriver förtydliganden eller begränsningar av dess bestämmelser genom medlemsstaternas nationella rätt, kan medlemsstaterna, i den utsträckning det är nödvändigt för samstämmigheten och för att göra de nationella bestämmelserna begripliga för de personer som de tillämpas på, införliva delar av denna förordning i nationell rätt.
- (9) Målen och principerna för direktiv 95/46/EG är fortfarande giltiga, men det har inte kunnat förhindra bristande enhetlighet i genomförandet av dataskyddet i olika delar av unionen, rättsosäkerhet eller allmänt spridda uppfattningar om att betydande risker kvarstår för fysiska personer, särskilt med avseende på användning av internet. Skillnader i nivån på skyddet av fysiska personers rättigheter och friheter, särskilt rätten till skydd av personuppgifter, vid behandling av personuppgifter i olika medlemsstater kan förhindra det fria flödet av personuppgifter över hela unionen. Dessa skillnader kan därför utgöra ett hinder för att bedriva ekonomisk verksamhet på unionsnivå, de kan snedvrída konkurrensen och hindra myndigheterna att fullgöra sina skyldigheter enligt unionsrätten. De varierande skyddsnivåerna beror på skillnader i genomförandet och tillämpningen av direktiv 95/46/EG.
- (10) För att säkra en enhetlig och hög skyddsnivå för fysiska personer och för att undanröja hindren för flödena av personuppgifter inom unionen bör nivån på skyddet av fysiska personers rättigheter och friheter vid behandling av personuppgifter vara likvärdig i alla medlemsstater. En konsekvent och enhetlig tillämpning av bestämmelserna om skydd av fysiska personers grundläggande rättigheter och friheter vid behandling av personuppgifter bör säkerställas i hela unionen. Vad gäller behandlingen av personuppgifter för att fullgöra en rättslig förpliktelse, för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning som utförs av den personuppgiftsansvarige, bör medlemsstaterna tillåtas att behålla eller införa nationella bestämmelser för att närmare fastställa hur bestämmelserna i denna förordning ska tillämpas. Jämte den allmänna och övergripande lagstiftning om dataskydd varigenom direktiv 95/46/EG genomförs har medlemsstaterna flera sektorsspecifika lagar på områden som kräver mer specifika bestämmelser. Denna förordning ger dessutom medlemsstaterna handlingsutrymme att specificera sina bestämmelser, även för behandlingen av särskilda kategorier av personuppgifter (nedan kallade *känsliga uppgifter*). Denna förordning utesluter inte att det i medlemsstaternas nationella rätt fastställs närmare omständigheter för specifika situationer där uppgifter behandlas, inbegripet mer exakta villkor för laglig behandling av personuppgifter.

- (11) Ett effektivt skydd av personuppgifter över hela unionen förutsätter att de registrerades rättigheter förstärks och specificeras och att de personuppgiftsansvarigas och personuppgiftsbiträdenas skyldigheter vid behandling av personuppgifter klargörs, samt att det finns likvärdiga befogenheter för övervakning och att det säkerställs att reglerna för skyddet av personuppgifter efterlevs och att sanktionerna för överträdelser är likvärdiga i medlemsstaterna.
- (12) I artikel 16.2 i EUF-fördraget bemyndigas Europaparlamentet och rådet att fastställa bestämmelser om skydd för fysiska personer när det gäller behandling av personuppgifter och bestämmelser om den fria rörligheten för personuppgifter.
- (13) För att säkerställa en enhetlig nivå för skyddet av fysiska personer över hela unionen och undvika avvikelser som hindrar den fria rörligheten av personuppgifter inom den inre marknaden behövs en förordning som skapar rättslig säkerhet och öppenhet för ekonomiska aktörer, däribland mikroföretag samt små och medelstora företag, och som ger fysiska personer i alla medlemsstater samma rättsligt verkställbara rättigheter och skyldigheter samt ålägger personuppgiftsansvariga och personuppgiftsbiträden samma ansvar, så att övervakningen av behandling av personuppgifter blir enhetlig, sanktionerna i alla medlemsstater likvärdiga och samarbetet mellan tillsynsmyndigheterna i olika medlemsstater effektivt. För att den inre marknaden ska fungera väl krävs att det fria flödet av personuppgifter inom unionen inte begränsas eller förbjuds av skäl som har anknytning till skydd för fysiska personer med avseende på behandling av personuppgifter. För att ta hänsyn till mikroföretagens samt de små och medelstora företagens särskilda situation innehåller denna förordning ett undantag för organisationer som sysselsätter färre än 250 personer med avseende på registerföring. Dessutom uppmanas unionens institutioner och organ samt medlemsstaterna och deras tillsynsmyndigheter att vid tillämpningen av denna förordning ta hänsyn till mikroföretagens samt de små och medelstora företagens särskilda behov. Begreppen mikroföretag samt små och medelstora företag bör bygga på artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG⁽¹⁾.
- (14) Det skydd som ska tillhandahållas enligt denna förordning bör tillämpas på fysiska personer, oavsett medborgarskap eller hemvist, med avseende på behandling av deras personuppgifter. Denna förordning omfattar inte behandling av personuppgifter rörande juridiska personer, särskilt företag som bildats som juridiska personer, exempelvis uppgifter om namn på och typ av juridisk person samt kontaktuppgifter.
- (15) För att förhindra att det uppstår en allvarlig risk för att reglerna kringgås bör skyddet för fysiska personer vara teknikneutralt och inte vara beroende av den teknik som används. Skyddet för fysiska personer bör vara tillämpligt på både automatiserad och manuell behandling av personuppgifter, om personuppgifterna ingår i eller är avsedda att ingå i ett register. Akter eller grupper av akter samt omslag till dessa, som inte är ordnade enligt särskilda kriterier, bör inte omfattas av denna förordning.
- (16) Denna förordning är inte tillämplig på frågor som rör skyddet av grundläggande rättigheter och friheter eller det fria flödet av personuppgifter på områden som inte omfattas av unionsrätten, såsom verksamhet rörande nationell säkerhet. Denna förordning är inte tillämplig på medlemsstaternas behandling av personuppgifter när de agerar inom ramen för unionens gemensamma utrikes- och säkerhetspolitik.
- (17) Europaparlamentets och rådets förordning (EG) nr 45/2001⁽²⁾ är tillämplig på den behandling av personuppgifter som sker i unionens institutioner, organ och byråer. Förordning (EG) nr 45/2001 och de av unionens övriga rättsakter som är tillämpliga på sådan behandling av personuppgifter bör anpassas till principerna och bestämmelserna i den här förordningen och tillämpas mot bakgrund av den här förordningen. För att tillhandahålla en stark och sammanhängande ram för dataskyddet inom unionen bör nödvändiga anpassningar av förordning (EG) nr 45/2001 göras när den här förordningen har antagits, så att de båda förordningarna kan tillämpas samtidigt.
- (18) Denna förordning är inte tillämplig på fysiska personers behandling av personuppgifter som ett led i verksamhet som är helt och hållet privat eller har samband med personens hushåll och därmed saknar koppling till yrkes- eller affärsmässig verksamhet. Privat verksamhet eller verksamhet som har samband med hushållet kan omfatta

⁽¹⁾ Kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (K(2003) 1422) (EUT L 124, 20.5.2003, s. 36).

⁽²⁾ Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).

korrespondens och innehav av adresser, aktivitet i sociala nätverk och internetverksamhet i samband med sådan verksamhet. Denna förordning är dock tillämplig på personuppgiftsansvariga eller personuppgiftsbiträden som tillhandahåller utrustning för behandling av personuppgifter för sådan privat verksamhet eller hushållsverksamhet.

- (19) Skyddet för fysiska personer när det gäller behöriga myndigheters behandling av personuppgifter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten och det fria flödet av sådana uppgifter, säkerställs på unionsnivå av en särskild unionsrättsakt. Därför bör denna förordning inte vara tillämplig på behandling av personuppgifter för dessa ändamål. Personuppgifter som myndigheter behandlar enligt denna förordning och som används för de ändamålen bör emellertid regleras genom en mer specifik unionsrättsakt, nämligen Europaparlamentets och rådets direktiv (EU) 2016/680⁽¹⁾. Medlemsstaterna får anförtro behöriga myndigheter i den mening som avses i direktiv (EU) 2016/680 uppgifter som inte nödvändigtvis utförs för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, så att behandlingen av personuppgifter för dessa andra ändamål, i den mån den omfattas av unionsrätten, omfattas av tillämpningsområdet för denna förordning.

Vad gäller dessa behöriga myndigheters behandling av personuppgifter för ändamål som omfattas av tillämpningsområdet för denna förordning, bör medlemsstaterna kunna bibehålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i denna förordning. I sådana bestämmelser får det fastställas mer specifika krav för dessa behöriga myndigheters behandling av personuppgifter för dessa andra ändamål, med beaktande av respektive medlemsstats konstitutionella, organisatoriska och administrativa struktur. När privata organs behandling av personuppgifter omfattas av tillämpningsområdet för denna förordning, bör denna förordning ge medlemsstaterna möjlighet att, under särskilda villkor, i lag begränsa vissa skyldigheter och rättigheter, om en sådan begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda särskilda viktiga intressen, däribland allmän säkerhet samt förebyggande, förhindrande, utredning, avslöjande och lagföring av brott eller verkställande av straffrättsliga påföljder eller skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten. Detta är exempelvis relevant i samband med bekämpning av penningtvätt eller verksamhet vid kriminaltekniska laboratorier.

- (20) Eftersom denna förordning bland annat gäller för verksamhet inom domstolar och andra rättsliga myndigheter, skulle det i unionsrätt eller medlemsstaternas nationella rätt kunna anges vilken behandling och vilka förfaranden för behandling som berörs när det gäller domstolars och andra rättsliga myndigheters behandling av personuppgifter. Tillsynsmyndigheternas behörighet bör inte omfatta domstolars behandling av personuppgifter när detta sker inom ramen för domstolarnas dömande verksamhet, i syfte att säkerställa domstolsväsendets oberoende när det utför sin rättsskipande verksamhet, inbegripet när det fattar beslut. Det bör vara möjligt att anförtro tillsynen över sådan behandling av uppgifter till särskilda organ inom medlemsstaternas rättsväsen, vilka framför allt bör säkerställa efterlevnaden av bestämmelserna i denna förordning, främja domstolsväsendets medvetenhet om sina skyldigheter enligt denna förordning och hantera klagomål relaterade till sådan behandling av uppgifter.
- (21) Denna förordning påverkar inte tillämpningen av Europaparlamentets och rådets direktiv 2000/31/EG⁽²⁾, särskilt bestämmelserna om tjänstelevererande mellanhanders ansvar i artiklarna 12–15 i det direktivet. Syftet med det direktivet är att bidra till att den inre marknaden fungerar väl genom att säkerställa fri rörlighet för informations-samhällets tjänster mellan medlemsstaterna.
- (22) All behandling av personuppgifter som sker inom ramen för arbetet på personuppgiftsansvarigas eller personuppgiftsbiträdens verksamhetsställen inom unionen bör ske i överensstämmelse med denna förordning, oavsett om behandlingen i sig äger rum inom unionen. Verksamhetsställe innebär det faktiska och reella utförandet av verksamhet med hjälp av en stabil struktur. Den rättsliga formen för en sådan struktur, oavsett om det är en filial eller ett dotterföretag med status som juridisk person, bör inte vara den avgörande faktorn i detta avseende.

⁽¹⁾ Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (se sidan 89 i detta nummer av EUT).

⁽²⁾ Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden ("Direktiv om elektronisk handel") (EUT L 178, 17.7.2000, s. 1).

- (23) För att fysiska personer inte ska fråntas det skydd som denna förordning ger dem bör sådan behandling av personuppgifter om registrerade personer som befinner sig i unionen vilken utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad inom unionen omfattas av denna förordning, om behandlingen avser utbudande av varor eller tjänster inom unionen till de registrerade, oavsett om detta är kopplat till en betalning. I syfte att avgöra om en personuppgiftsansvarig eller ett personuppgiftsbiträde erbjuder varor eller tjänster till registrerade som befinner sig i unionen bör man fastställa om det är uppenbart att den personuppgiftsansvarige eller personuppgiftsbiträdet avser att erbjuda tjänster till registrerade i en eller flera av unionens medlemsstater. Medan enbart åtkomlighet till den personuppgiftsansvariges, personuppgiftsbitrådets eller en mellanhands webbplats i unionen, till en e-postadress eller andra kontaktuppgifter eller användning av ett språk som allmänt används i det tredjeland där den personuppgiftsansvarige är etablerad inte är tillräckligt för att fastställa en sådan avsikt, kan faktorer som användning av ett språk eller en valuta som allmänt används i en eller flera medlemsstater med möjlighet att beställa varor och tjänster på detta andra språk, eller omnämnande av kunder eller användare som befinner sig i unionen, göra det uppenbart att den personuppgiftsansvarige avser att erbjuda varor eller tjänster till registrerade inom unionen.
- (24) Den behandling av personuppgifter som avser registrerade som befinner sig i unionen som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad i unionen bör också omfattas av denna förordning, om den hör samman med övervakningen av de registrerade personernas beteende när de befinner sig i unionen. För att avgöra huruvida en viss behandling kan anses övervaka beteendet hos registrerade, bör det fastställas om fysiska personer spåras på internet, och om personuppgifterna därefter behandlas med hjälp av teknik som profilerar fysiska personer, i synnerhet för att fatta beslut rörande honom eller henne eller för att analysera eller förutsäga hans eller hennes personliga preferenser, beteende och attityder.
- (25) Om medlemsstaternas nationella rätt är tillämplig i kraft av folkrätten, bör denna förordning också vara tillämplig på personuppgiftsansvariga som inte är etablerade inom unionen, exempelvis i en medlemsstats diplomatiska beskickning eller konsulat.
- (26) Principerna för dataskyddet bör gälla all information som rör en identifierad eller identifierbar fysisk person. Personuppgifter som har pseudonymiserats och som skulle kunna tillskrivas en fysisk person genom att kompletterande uppgifter används bör anses som uppgifter om en identifierbar fysisk person. För att avgöra om en fysisk person är identifierbar bör man beakta alla hjälpmedel, som t.ex. utgallring, som, antingen av den personuppgiftsansvarige eller av en annan person, rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen. För att fastställa om hjälpmedel med rimlig sannolikhet kan komma att användas för att identifiera den fysiska personen bör man beakta samtliga objektiva faktorer, såsom kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten för behandlingen som den tekniska utvecklingen. Principerna för dataskyddet bör därför inte gälla för anonym information, nämligen information som inte hänför sig till en identifierad eller identifierbar fysisk person, eller för personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte eller inte längre är identifierbar. Denna förordning berör därför inte behandling av sådan anonym information, vilket inbegriper information för statistiska ändamål eller forskningsändamål.
- (27) Denna förordning gäller inte behandling av personuppgifter rörande avlidna personer. Medlemsstaterna får fastställa bestämmelser för behandlingen av personuppgifter rörande avlidna personer.
- (28) Tillämpningen av pseudonymisering av personuppgifter kan minska riskerna för de registrerade som berörs och hjälpa personuppgiftsansvariga och personuppgiftsbiträden att fullgöra sina skyldigheter i fråga om dataskydd. Ett uttryckligt införande av *pseudonymisering* i denna förordning är inte avsett att utesluta andra åtgärder för dataskydd.
- (29) För att skapa incitament för tillämpning av pseudonymisering vid behandling av personuppgifter bör åtgärder för pseudonymisering som samtidigt medger en allmän analys vara möjliga inom samma personuppgiftsansvarigs verksamhet, när den personuppgiftsansvarige har vidtagit de tekniska och organisatoriska åtgärder som är nödvändiga för att se till att denna förordning genomförs för berörd uppgiftsbehandling och att kompletterande uppgifter för tillskrivning av personuppgifterna till en specifik registrerad person förvaras separat. Den personuppgiftsansvarige som behandlar personuppgifterna bör ange behöriga personer inom samma personuppgiftsansvarigs verksamhet.

- (30) Fysiska personer kan knytas till nätidentifierare som lämnas av deras utrustning, applikationer, verktyg och protokoll, t.ex. ip-adresser, kakor eller andra identifierare, som radiofrekvensetiketter. Detta kan efterlämna spår som, särskilt i kombination med unika identifierare och andra uppgifter som tas emot av serverna, kan användas för att skapa profiler för fysiska personer och identifiera dem.
- (31) Offentliga myndigheter som för sin myndighetsutövning mottar personuppgifter i enlighet med en rättslig förpliktelse, t.ex. skatte- och tullmyndigheter, finansutredningsgrupper, oberoende administrativa myndigheter eller finansmarknadsmyndigheter med ansvar för reglering och övervakning av värdepappersmarknader, bör inte betraktas som mottagare om de tar emot personuppgifter som är nödvändiga för utförandet av en särskild utredning av allmänt intresse, i enlighet med unionsrätten eller medlemstaternas nationella rätt. Offentliga myndigheters begäranden om att uppgifter ska lämnas ut ska alltid vara skriftliga och motiverade, läggas fram i enskilda fall och inte gälla hela register eller leda till att register kopplas samman. Dessa offentliga myndigheters behandling av personuppgifter bör ske i överensstämmelse med de bestämmelser för dataskydd som är tillämpliga på behandlingens ändamål.
- (32) Samtycke bör lämnas genom en entydig bekräftande handling som innebär ett frivilligt, specifikt, informerat och otvetydigt medgivande från den registrerades sida om att denne godkänner behandling av personuppgifter rörande honom eller henne, som t.ex. genom en skriftlig, inklusive elektronisk, eller muntlig förklaring. Detta kan innebära att en ruta kryssas i vid besök på en internetsida, genom val av inställningsalternativ för tjänster på informationssamhällets område eller genom någon annan förklaring eller något annat beteende som i sammanhanget tydligt visar att den registrerade godtar den avsedda behandlingen av sina personuppgifter. Tystnad, på förhand ikryssade rutor eller inaktivitet bör därför inte utgöra samtycke. Samtycket bör gälla all behandling som utförs för samma ändamål. Om behandlingen tjänar flera olika syften, bör samtycke ges för samtliga syften. Om den registrerade ska lämna sitt samtycke efter en elektronisk begäran, måste denna vara tydlig och koncis och får inte onödigtvis störa användningen av den tjänst som den avser.
- (33) Det är ofta inte möjligt att fullt ut identifiera syftet med en behandling av personuppgifter för vetenskapliga forskningsändamål i samband med insamlingen av uppgifter. Därför bör registrerade kunna ge sitt samtycke till vissa områden för vetenskaplig forskning, när vedertagna etiska standarder för vetenskaplig forskning iaktas. Registrerade bör ha möjlighet att endast lämna sitt samtycke till vissa forskningsområden eller delar av forskningsprojekt i den utsträckning det avsedda syftet medger detta.
- (34) Genetiska uppgifter bör definieras som personuppgifter som rör en fysisk persons nedärvda eller förvärvade genetiska kännetecken, vilka framgår av en analys av ett biologiskt prov från den fysiska personen i fråga, framför allt kromosom-, DNA- eller RNA-analys eller av en annan form av analys som gör det möjligt att inhämta motsvarande information.
- (35) Personuppgifter om hälsa bör innefatta alla de uppgifter som hänför sig till en registrerad persons hälsotillstånd som ger information om den registrerades tidigare, nuvarande eller framtida fysiska eller psykiska hälsotillstånd. Detta inbegriper uppgifter om den fysiska personen som insamlats i samband med registrering för eller tillhandahållande av hälso- och sjukvårdstjänster till den fysiska personen enligt Europaparlamentets och rådets direktiv 2011/24/EU⁽¹⁾, ett nummer, en symbol eller ett kännetecken som den fysiska personen tilldelats för att identifiera denne för hälso- och sjukvårdsändamål, uppgifter som härrör från tester eller undersökning av en kroppsdelen eller kroppssubstans, däribland genetiska uppgifter och biologiska prov, och andra uppgifter om exempelvis sjukdom, funktionshinder, sjukdomsrisk, sjukdomshistoria, klinisk behandling eller den registrerades fysiologiska eller biomedicinska tillstånd, oberoende av källan, exempelvis från en läkare eller från annan sjukvårdspersonal, ett sjukhus, en medicinteknisk produkt eller ett diagnostiskt in vitro-test.
- (36) Den personuppgiftsansvariges huvudsakliga verksamhetsställe i unionen bör vara den plats i unionen där den personuppgiftsansvarige har sin centrala förvaltning, såvida inte beslut om ändamålen och medlen för behandling av personuppgifter fattas vid ett annat av den personuppgiftsansvariges verksamhetsställen i unionen; i sådant fall

⁽¹⁾ Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).

bör det andra verksamhetsstället anses vara det huvudsakliga verksamhetsstället. En personuppgiftsansvarigs huvudsakliga verksamhetsställe inom unionen bör avgöras med beaktande av objektiva kriterier och bör inbegripa den faktiska och reella ledning som fattar de huvudsakliga besluten vad avser ändamål och medel för behandlingen med hjälp av en stabil struktur. Detta kriterium bör inte vara avhängigt av om behandlingen av personuppgifter utförs på detta ställe. Att tekniska medel och teknik för behandling av personuppgifter eller behandlingsverksamhet finns och används visar i sig inte att det rör sig om ett huvudsakligt verksamhetsställe och utgör därför inte avgörande kriterier för ett huvudsakligt verksamhetsställe. Personuppgiftsbitrådets huvudsakliga verksamhetsställe bör vara den plats i unionen där denne har sin centrala förvaltning eller, om denne inte har någon central förvaltning inom unionen, den plats inom unionen där den huvudsakliga behandlingen sker. I fall som omfattar både en personuppgiftsansvarig och ett personuppgiftsbiträde bör den behöriga ansvariga tillsynsmyndigheten fortfarande vara tillsynsmyndigheten i den medlemsstat där den personuppgiftsansvarige har sitt huvudsakliga verksamhetsställe, men den tillsynsmyndighet som gäller för personuppgiftsbitrådet bör betraktas som en berörd tillsynsmyndighet och den tillsynsmyndigheten bör delta i det samarbetsförfarande som föreskrivs i denna förordning. Om utkastet till beslut endast gäller den personuppgiftsansvarige, bör tillsynsmyndigheterna i den eller de medlemsstater där personuppgiftsbitrådet har ett eller flera verksamhetsställen inte under några omständigheter betraktas som berörda tillsynsmyndigheter. Om behandlingen utförs av en koncern bör det kontrollerande företags huvudsakliga verksamhetsställe betraktas som koncernens huvudsakliga verksamhetsställe, utom då behandlingens ändamål och de medel med vilka den utförs fastställs av ett annat företag.

- (37) En koncern bör innefatta ett kontrollerande företag och de företag som detta företag kontrollerar (kontrollerade företag), varvid det kontrollerande företaget bör vara det företag som kan utöva ett dominerande inflytande på de övriga företagen i kraft av exempelvis ägarskap, finansiellt deltagande eller de bestämmelser som det regleras av eller befogenheten att införa regler som rör personuppgiftsskyddet. Ett företag med kontroll över behandlingen av personuppgifter vid företag som är underställda detta företag bör, tillsammans med dessa företag, anses utgöra en koncern.
- (38) Barns personuppgifter förtjänar särskilt skydd, eftersom barn kan vara mindre medvetna om berörda risker, följder och skyddsåtgärder samt om sina rättigheter när det gäller behandling av personuppgifter. Sådant särskilt skydd bör i synnerhet gälla användningen av barns personuppgifter i marknadsföringssyfte eller för att skapa personlighets- eller användarprofiler samt insamling av personuppgifter med avseende på barn när tjänster som erbjuds direkt till barn utnyttjas. Samtycke från den person som har föräldraansvar över ett barn bör inte krävas för förebyggande eller rådgivande tjänster som erbjuds direkt till barn.
- (39) Varje behandling av personuppgifter måste vara laglig och rättvis. Det bör vara klart och tydligt för fysiska personer hur personuppgifter som rör dem insamlas, används, konsulteras eller på annat sätt behandlas samt i vilken utsträckning personuppgifterna behandlas eller kommer att behandlas. Öppenhetsprincipen kräver att all information och kommunikation i samband med behandlingen av dessa personuppgifter är lättillgänglig och lättbegriplig samt att ett klart och tydligt språk används. Den principen gäller framför allt informationen till registrerade om den personuppgiftsansvariges identitet och syftet med behandlingen samt ytterligare information för att sörja för en rättvis och öppen behandling för berörda fysiska personer och deras rätt att erhålla bekräftelse på och meddelande om vilka personuppgifter rörande dem som behandlas. Fysiska personer bör göras medvetna om risker, regler, skyddsåtgärder och rättigheter i samband med behandlingen av personuppgifter och om hur de kan utöva sina rättigheter med avseende på behandlingen. De specifika ändamål som personuppgifterna behandlas för bör vara tydliga och legitima och ha bestämts vid den tidpunkt då personuppgifterna samlades in. Personuppgifterna bör vara adekvata, relevanta och begränsade till vad som är nödvändigt för de ändamål som de behandlas för. Detta kräver i synnerhet att det tillses att den period under vilken personuppgifterna lagras är begränsad till ett strikt minimum. Personuppgifter bör endast behandlas om syftet med behandlingen inte rimligen kan uppnås genom andra medel. För att säkerställa att personuppgifter inte sparas längre än nödvändigt bör den personuppgiftsansvarige införa tidsfrister för radering eller för regelbunden kontroll. Alla rimliga åtgärder bör vidtas för att rätta eller radera felaktiga uppgifter. Personuppgifter bör behandlas på ett sätt som säkerställer lämplig säkerhet och konfidentialitet för personuppgifterna samt förhindrar obehörigt tillträde till och obehörig användning av personuppgifter och den utrustning som används för behandlingen.
- (40) För att behandling ska vara laglig bör personuppgifterna behandlas efter samtycke från den berörda registrerade eller på någon annan legitim grund som fastställts i lag, antingen i denna förordning eller i annan unionsrätt eller

medlemsstaternas nationella rätt enligt denna förordning, vilket inbegriper att de rättsliga skyldigheter som åligger den personuppgiftsansvarige måste fullgöras eller att ett avtal i vilket den registrerade är part måste genomföras eller att åtgärder på begäran av den registrerade måste vidtas innan avtalet ingås.

- (41) När det i denna förordning hänvisas till en rättslig grund eller lagstiftningsåtgärd, innebär detta inte nödvändigtvis en lagstiftningsakt antagen av ett parlament, utan att detta påverkar krav som uppställs i den konstitutionella ordningen i den berörda medlemsstaten. En sådan rättslig grund eller lagstiftningsåtgärd bör dock vara tydlig och precis och dess tillämpning bör vara förutsägbar för personer som omfattas av den, i enlighet med rättspraxis vid Europeiska unionens domstol (nedan kallad *domstolen*) och Europeiska domstolen för de mänskliga rättigheterna.
- (42) När behandling sker efter samtycke från registrerade, bör personuppgiftsansvariga kunna visa att de registrerade har lämnat sitt samtycke till behandlingen. I synnerhet vid skriftliga förklaringar som rör andra frågor bör det finnas skyddsåtgärder som säkerställer att de registrerade är medvetna om att samtycke ges och om hur långt samtycket sträcker sig. I enlighet med rådets direktiv 93/13/EEG⁽¹⁾ bör en förklaring om samtycke som den personuppgiftsansvarige i förväg formulerat tillhandahållas i en begriplig och lätt tillgänglig form, med användning av ett klart och tydligt språk och utan oskäligen villkor. För att samtycket ska vara informerat bör den registrerade känna till åtminstone den personuppgiftsansvariges identitet och syftet med den behandling för vilken personuppgifterna är avsedda. Samtycke bör inte betraktas som frivilligt om den registrerade inte har någon genuin eller fri valmöjlighet eller inte utan problem kan vägra eller ta tillbaka sitt samtycke.
- (43) För att säkerställa att samtycket lämnas frivilligt bör det inte utgöra giltig rättslig grund för behandling av personuppgifter i ett särskilt fall där det råder betydande ojämlikhet mellan den registrerade och den personuppgiftsansvarige, särskilt om den personuppgiftsansvarige är en offentlig myndighet och det därför är osannolikt att samtycket har lämnats frivilligt när det gäller alla förhållanden som denna särskilda situation omfattar. Samtycke antas inte vara frivilligt om det inte medger att separata samtycken lämnas för olika behandlingar av personuppgifter, trots att detta är lämpligt i det enskilda fallet, eller om genomförandet av ett avtal – inbegripet tillhandahållandet av en tjänst – är avhängigt av samtycket, trots att samtycket inte är nödvändigt för ett sådant genomförande.
- (44) Behandling bör vara laglig när den är nödvändig i samband med avtal eller när det finns en avsikt att ingå ett avtal.
- (45) Behandling som grundar sig på en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller behandling som krävs för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning, bör ha en grund i unionsrätten eller i en medlemsstats nationella rätt. Denna förordning medför inte något krav på en särskild lag för varje enskild behandling. Det kan räcka med en lag som grund för flera behandlingar som bygger på en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller om behandlingen krävs för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning. Behandlingens syfte bör också fastställas i unionsrätten eller i medlemsstaternas nationella rätt. Därtill skulle man genom denna grund kunna ange denna förordnings allmänna villkor för laglig personuppgiftsbehandling och precisera kraven för att fastställa vem den personuppgiftsansvarige är, vilken typ av personuppgifter som ska behandlas, vilka registrerade som berörs, de enheter till vilka personuppgifterna får lämnas ut, ändamålsbegränsningar, lagringstid samt andra åtgärder för att tillförsäkra en laglig och rättvis behandling. Unionsrätten eller medlemsstaternas nationella rätt bör också reglera frågan huruvida en personuppgiftsansvarig som utför en uppgift av allmänt intresse eller som ett led i myndighetsutövning ska vara en offentlig myndighet eller någon annan fysisk eller juridisk person som omfattas av offentlig-rättslig lagstiftning eller, om detta motiveras av allmänintresset, vilket inbegriper hälso- och sjukvårdsändamål, såsom folkhälsa och socialt skydd och förvaltning av hälso- och sjukvårdstjänster, av civilrättslig lagstiftning, exempelvis en yrkesorganisation.
- (46) Behandling av personuppgifter bör även anses laglig när den är nödvändig för att skydda ett intresse som är av avgörande betydelse för den registrerades eller en annan fysisk persons liv. Behandling av personuppgifter på

(¹) Rådets direktiv 93/13/EEG av den 5 april 1993 om oskäligen villkor i konsumentavtal (EGTL 95, 21.4.1993, s. 29).

grundval av en annan fysisk persons grundläggande intressen bör i princip endast äga rum om behandlingen inte uppenbart kan ha en annan rättslig grund. Vissa typer av behandling kan tjäna både viktiga allmänintressen och intressen som är av grundläggande betydelse för den registrerade, till exempel när behandlingen är nödvändig av humanitära skäl, bland annat för att övervaka epidemier och deras spridning eller i humanitära nödsituationer, särskilt vid naturkatastrofer eller katastrofer orsakade av människan.

- (47) En personuppgiftsansvarigs berättigade intressen, inklusive intressena för en personuppgiftsansvarig till vilken personuppgifter får lämnas ut, eller för en tredje part, kan utgöra rättslig grund för behandling, på villkor att de registrerades intressen eller grundläggande rättigheter och friheter inte väger tyngre, med beaktande av de registrerades rimliga förväntningar till följd av förhållandet till den personuppgiftsansvarige. Ett sådant berättigat intresse kan till exempel finnas när det föreligger ett relevant och lämpligt förhållande mellan den registrerade och den personuppgiftsansvarige i sådana situationer som att den registrerade är kund hos eller arbetar för den personuppgiftsansvarige. Ett berättigat intresse kräver under alla omständigheter en noggrann bedömning, som inbegriper huruvida den registrerade vid tidpunkten för inhämtandet av personuppgifter och i samband med detta rimligen kan förvänta sig att en uppgiftsbehandling för detta ändamål kan komma att ske. Den registrerades intressen och grundläggande rättigheter skulle i synnerhet kunna väga tyngre än den personuppgiftsansvariges intressen, om personuppgifter behandlas under omständigheter där den registrerade inte rimligen kan förvänta sig någon ytterligare behandling. Med tanke på att det är lagstiftarens sak att genom lagstiftning tillhandahålla den rättsliga grunden för de offentliga myndigheternas behandling av personuppgifter, bör den rättsliga grunden inte gälla den behandling de utför som ett led i fullgörandet av sina uppgifter. Sådant behandling av personuppgifter som är absolut nödvändig för att förhindra bedrägerier utgör också ett berättigat intresse för berörd personuppgiftsansvarig. Behandling av personuppgifter för direktmarknadsföring kan betraktas som ett berättigat intresse.
- (48) Personuppgiftsansvariga som ingår i en koncern eller institutioner som är underställda ett centralt organ kan ha ett berättigat intresse att överföra personuppgifter inom koncernen för interna administrativa ändamål, bland annat för behandling av kunders eller anställdas personuppgifter. De allmänna principerna för överföring av personuppgifter, inom en koncern, till företag i tredjeland påverkas inte.
- (49) Behandling av personuppgifter utgör ett berättigat intresse för berörd personuppgiftsansvarig i den mån den är absolut nödvändig och proportionell för att säkerställa nät- och informationssäkerhet, dvs. förmågan hos ett nät eller ett informationssystem att vid en viss tillförlitlighetsnivå tåla olyckshändelser, olagliga handlingar eller illvilligt uppträdande som äventyrar tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade eller överförda personuppgifter och säkerheten hos besläktade tjänster som tillhandahålls av – eller är tillgängliga via – dessa nät och system, av myndigheter, incidenthanteringsorganisationer (Cert), enheter för hantering av datasäkerhetsincidenter, tillhandahållare av elektroniska kommunikationsnät och kommunikationstjänster och tillhandahållare av säkerhetsteknik och säkerhetstjänster. Detta skulle t.ex. kunna innefatta att förhindra obehörigt tillträde till elektroniska kommunikationsnät och felaktig kodfördelning och att sätta stopp för överbelastningsattacker och skador på datasystem och elektroniska kommunikationssystem.
- (50) Behandling av personuppgifter för andra ändamål än de för vilka de ursprungligen samlades in bör endast vara tillåten, när detta är förenligt med de ändamål för vilka personuppgifterna ursprungligen samlades in. I dessa fall krävs det inte någon annan separat rättslig grund än den med stöd av vilken insamlingen av personuppgifter medgavs. Om behandlingen är nödvändig för att fullgöra en uppgift av allmänt intresse eller som ett led i myndighetsutövning som den personuppgiftsansvarige har fått i uppgift att utföra, kan unionsrätten eller medlemsstaternas nationella rätt fastställa och närmare ange för vilka uppgifter och syften ytterligare behandling bör betraktas som förenlig och laglig. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör betraktas som förenlig och laglig behandling av uppgifter. Den rättsliga grund för behandling av personuppgifter som återfinns i unionsrätten eller i medlemsstaternas nationella rätt kan också utgöra en rättslig grund för ytterligare behandling. För att fastställa om ett ändamål med den ytterligare behandlingen är förenligt med det ändamål för vilket personuppgifterna ursprungligen insamlades bör den personuppgiftsansvarige, efter att ha uppfyllt alla krav vad beträffar den ursprungliga behandlingens lagenlighet, bland annat beakta alla kopplingar mellan dessa ändamål och ändamålen med den avsedda ytterligare behandlingen, det sammanhang inom vilket personuppgifterna insamlats, särskilt de registrerades rimliga förväntningar till följd av förhållandet till den personuppgiftsansvarige i fråga om den

art, den planerade ytterligare behandlingens konsekvenser för de registrerade samt förekomsten av lämpliga skyddsåtgärder för både den ursprungliga och den planerade ytterligare behandlingen.

Om den registrerade har gett sitt medgivande eller behandlingen grundar sig på unionsrätten eller på medlemsstaternas nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa i synnerhet viktiga mål av allmänt intresse, bör den personuppgiftsansvarige tillåtas att behandla personuppgifterna ytterligare, oavsett om detta är förenligt med ändamålen eller inte. Under alla omständigheter bör tillämpningen av principerna i denna förordning, särskilt informationen till den registrerade om dessa andra ändamål och om dennes rättigheter, inbegripet rätten att göra invändningar, säkerställas. Om den personuppgiftsansvarige anmäler möjliga brott eller hot mot den allmänna säkerheten och i enskilda fall eller i flera fall som rör samma brott eller hot mot den allmänna säkerheten överför dessa personuppgifter till en behörig myndighet, ska detta betraktas som att den personuppgiftsansvarige agerar i ett berättigat intresse. Sådan överföring i den personuppgiftsansvariges berättigade intresse eller ytterligare behandling av personuppgifter bör emellertid vara förbjuden, om behandlingen inte är förenlig med lagstadgad eller yrkesmässig tystnadsplikt eller annan bindande tystnadsplikt.

- (51) Personuppgifter som till sin natur är särskilt känsliga med hänsyn till grundläggande rättigheterna och friheter bör åtnjuta särskilt skydd, eftersom behandling av sådana uppgifter kan innebära betydande risker för de grundläggande rättigheterna och friheterna. Dessa personuppgifter bör även inbegripa personuppgifter som avslöjar ras eller etniskt ursprung, varvid användningen av termen *ras* i denna förordning inte innebär att unionen godtar teorier som söker fastställa förekomsten av skilda människoraser. Behandling av foton bör inte systematiskt anses utgöra behandling av särskilda kategorier av personuppgifter, eftersom foton endast definieras som biometriska uppgifter när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person. Sådana personuppgifter bör inte behandlas, såvida inte behandling medges i särskilda fall som fastställs i denna förordning, med beaktande av att det i medlemsstaternas lagstiftning får införas särskilda bestämmelser om dataskydd för att anpassa tillämpningen av bestämmelserna i denna förordning i syfte att fullgöra en rättslig skyldighet eller en uppgift av allmänt intresse eller som ett led i myndighetsutövning som den personuppgiftsansvarige har fått i uppgift att utföra. Utöver de särskilda kraven för sådan behandling, bör de allmänna principerna och andra bestämmelser i denna förordning tillämpas, särskilt när det gäller villkoren för laglig behandling. Undantag från det allmänna förbudet att behandla sådana särskilda kategorier av personuppgifter bör uttryckligen fastställas, bland annat om den registrerade lämnar sitt uttryckliga samtycke eller för att tillgodose specifika behov, i synnerhet när behandlingen utförs inom ramen för legitima verksamheter som bedrivs av vissa sammanslutningar eller stiftelser i syfte att göra det möjligt att utöva grundläggande friheter.
- (52) Undantag från förbudet att behandla särskilda kategorier av personuppgifter bör även tillåtas om de föreskrivs i unionsrätten eller i medlemsstaternas nationella rätt och underkastas lämpliga skyddsåtgärder för att skydda personuppgifter och övriga grundläggande rättigheter, när allmänintresset motiverar detta, i synnerhet i fråga om behandling av personuppgifter inom ramen för arbetsrätt och sociallagstiftning, däribland pensioner, och för hälsosäkerhetsändamål, övervaknings- och varningssyften, förebyggande eller kontroll av smittsamma sjukdomar och andra allvarliga hot mot hälsan. Detta undantag får göras för hälsoändamål, inbegripet folkhälsa och förvaltningen av hälso- och sjukvårdstjänster, särskilt för att säkerställa kvalitet och kostnadseffektivitet i de förfaranden som används vid prövningen av ansökningar om förmåner och tjänster inom sjukförsäkringssystemet, eller för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Genom undantag bör man även tillåta behandling av sådana personuppgifter där så krävs för fastställande, utövande eller försvar av rättsliga anspråk, oavsett om detta sker inom ett domstolsförfarande eller inom ett administrativt eller ett utomrättsligt förfarande.
- (53) Särskilda kategorier av personuppgifter som förtjänar ett mer omfattande skydd bör endast behandlas i hälsorelaterade syften om detta krävs för att uppnå dessa syften och gagnar fysiska personer och samhället i stort, särskilt inom ramen för förvaltningen av tjänster för hälso- och sjukvård och social omsorg och deras system, inbegripet behandling som utförs av förvaltningen och centrala nationella hälsovårdsmyndigheter av sådana uppgifter för syften som hör samman med kvalitetskontroll, information om förvaltningen samt allmän nationell och lokal tillsyn över hälso- och sjukvårdssystemet och systemet för social omsorg och säkerställande av kontinuitet inom hälso- och sjukvård och social omsorg samt gränsöverskridande hälso- och sjukvård eller hälsosäkerhet, syften som hör samman med övervakning samt varningssyften eller för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål som baseras på unionsrätten eller på medlemsstaternas nationella rätt, vilka måste ha ett syfte av allmänt intresse, samt studier som genomförs av allmänt intresse på folkhälsoområdet. Denna förordning bör därför innehålla harmoniserade villkor för behandling av särskilda kategorier av personuppgifter om hälsa, vad gäller särskilda behov, i synnerhet när behandlingen av uppgifterna utförs för vissa hälsorelaterade syften av personer som enligt lag är underkastade

yrkesmässig tystnadsplikt. Unionsrätten eller medlemsstaternas nationella rätt bör föreskriva särskilda och lämpliga åtgärder som skyddar fysiska personers grundläggande rättigheter och personuppgifter. Medlemsstaterna bör få behålla eller införa ytterligare villkor, även begränsningar, för behandlingen av genetiska eller biometriska uppgifter eller uppgifter om hälsa. Detta bör emellertid inte hindra det fria flödet av personuppgifter inom unionen, när villkoren tillämpas på gränsöverskridande behandling av sådana uppgifter.

- (54) På folkhälsoområdet kan det bli nödvändigt att med hänsyn till ett allmänt intresse behandla särskilda kategorier av personuppgifter utan att den registrerades samtycke inhämtas. Sådan behandling bör förutsätta lämpliga och särskilda åtgärder för att skydda fysiska personers rättigheter och friheter. I detta sammanhang bör *folkhälsa* tolkas enligt definitionen i Europaparlamentets och rådets förordning (EG) nr 1338/2008 ⁽¹⁾, nämligen alla aspekter som rör hälsosituationen, dvs. allmänhetens hälsotillstånd, inbegripet sjuklighet och funktionshinder, hälsans bestämningfaktorer, hälso- och sjukvårdsbehov, resurser inom hälso- och sjukvården, tillhandahållande av och allmän tillgång till hälso- och sjukvård, utgifter för och finansiering av hälso- och sjukvården samt dödsorsaker. Sådan behandling av uppgifter om hälsa av allmänt intresse bör inte innebära att personuppgifter behandlas för andra ändamål av tredje part, exempelvis arbetsgivare eller försäkrings- och bankföretag.
- (55) Myndigheters behandling av personuppgifter på officiellt erkända religiösa sammanslutningars vägnar i syften som fastställs i grundlag eller i folkrätten anses också grunda sig på ett allmänt intresse.
- (56) Om det för att det demokratiska systemet ska fungera i samband med allmänna val är nödvändigt att politiska partier i vissa medlemsstater samlar in personuppgifter om fysiska personers politiska uppfattningar, får behandling av sådana uppgifter tillåtas med hänsyn till ett allmänt intresse, på villkor att lämpliga skyddsåtgärder fastställs.
- (57) Om de personuppgifter som behandlas av en personuppgiftsansvarig inte gör det möjligt för denne att identifiera en fysisk person, bör den personuppgiftsansvarige inte vara tvungen att skaffa ytterligare information för att kunna identifiera den registrerade, om ändamålet endast är att följa någon av bestämmelserna i denna förordning. Den personuppgiftsansvarige bör dock inte vägra att ta emot kompletterande uppgifter som den registrerade lämnat som stöd för utövandet av sina rättigheter. Identifiering bör omfatta digital identifiering av en registrerad, till exempel genom en autentiseringsmekanism, exempelvis samma identifieringsinformation som används av den registrerade för att logga in på den nättjänst som tillhandahålls av den personuppgiftsansvarige.
- (58) Öppenhetsprincipen kräver att all information som riktar sig till allmänheten eller till registrerade är kortfattad, lättåtkomlig och lättbegriplig samt utformad på ett tydligt och enkelt språk samt att man vid behov använder visualisering. Denna information kan ges elektroniskt, exempelvis på en webbplats, när den riktar sig till allmänheten. Detta är särskilt relevant i situationer där mängden olika aktörer och den tekniska komplexiteten gör det svårt för den registrerade att veta och förstå om personuppgifter som rör honom eller henne samlas in, vem som gör det och för vilket syfte, exempelvis i fråga om reklam på nätet. Eftersom barn förtjänar särskilt skydd, bör all information och kommunikation som riktar sig till barn utformas på ett tydligt och enkelt språk som barnet lätt kan förstå.
- (59) Förfaranden bör fastställas som gör det lättare för registrerade att utöva sina rättigheter enligt denna förordning, inklusive mekanismer för att begära och i förekommande fall kostnadsfritt få tillgång till och erhålla rättelse eller radering av personuppgifter samt för att utöva rätten att göra invändningar. Den personuppgiftsansvarige bör också tillhandahålla hjälpmedel för elektroniskt ingivna framställningar, särskilt i fall då personuppgifter behandlas elektroniskt. Personuppgiftsansvariga bör utan onödigt dröjsmål och senast inom en månad vara skyldiga att besvara registrerades önskemål och lämna en motivering, om de inte avser att uppfylla sådana önskemål.

⁽¹⁾ Europaparlamentets och rådets förordning (EG) nr 1338/2008 av den 16 december 2008 om gemenskapsstatistik om folkhälsa och hälsa och säkerhet i arbetet (EUTL 354, 31.12.2008, s. 70).

- (60) Principerna om rättvis och öppen behandling fordrar att den registrerade informeras om att behandling sker och syftet med den. Den personuppgiftsansvarige bör till den registrerade lämna all ytterligare information som krävs för att säkerställa en rättvis och öppen behandling, med beaktande av personuppgiftsbehandlingens specifika omständigheter och sammanhang. Dessutom bör den registrerade informeras om förekomsten av profilering samt om konsekvenserna av sådan profilering. Om personuppgifterna samlas in från den registrerade, bör denne även informeras om huruvida han eller hon är skyldig att tillhandahålla personuppgifterna och om konsekvenserna om han eller hon inte lämnar dem. Denna information får tillhandahållas kombinerad med standardiserade symboler för att ge en överskådlig, begriplig, lättläst och meningsfull överblick över den planerade behandlingen. Om sådana symboler visas elektroniskt bör de vara maskinläsbara.
- (61) Information om behandling av personuppgifter som rör den registrerade bör lämnas till honom eller henne vid den tidpunkt då personuppgifterna samlas in från den registrerade eller, om personuppgifterna erhålls direkt från en annan källa, inom en rimlig period, beroende på omständigheterna i fallet. Om personuppgifter legitimt kan lämnas ut till en annan mottagare, bör de registrerade informeras första gången personuppgifterna lämnas ut till denna mottagare. Om den personuppgiftsansvarige avser att behandla personuppgifter för ett annat ändamål än det för vilket uppgifterna insamlades, bör denne före ytterligare behandling informera den registrerade om detta andra syfte och lämna annan nödvändig information. Om personuppgifternas ursprung inte kan meddelas den registrerade på grund av att olika källor har använts, bör allmän information ges.
- (62) Det är dock inte nödvändigt att införa någon skyldighet att tillhandahålla information, om den registrerade redan innehar denna information, om registreringen eller utlämnandet av personuppgifterna uttryckligen föreskrivs i lag eller om det visar sig vara omöjligt eller skulle medföra orimliga ansträngningar att tillhandahålla den registrerade informationen. Det sistnämnda skulle särskilt kunna vara fallet om behandlingen sker för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. I detta avseende bör antalet registrerade, uppgifternas ålder och lämpliga skyddsåtgärder beaktas.
- (63) Den registrerade bör ha rätt att få tillgång till personuppgifter som insamlats om denne samt på enkelt sätt och med rimliga intervall kunna utöva denna rätt, för att vara medveten om att behandling sker och kunna kontrollera att den är laglig. Detta innefattar rätten för registrerade att få tillgång till uppgifter om sin hälsa, exempelvis uppgifter i läkarjournaler med t.ex. diagnoser, undersökningsresultat, bedömningar av behandlande läkare och eventuella vårdbehandlingar eller interventioner. Alla registrerade bör därför ha rätt att få kännedom och underrättelse om framför allt orsaken till att personuppgifterna behandlas, om möjligt vilken tidsperiod behandlingen pågår, vilka som mottar personuppgifterna, bakomliggande logik i samband med automatisk behandling av personuppgifter och, åtminstone när behandlingen bygger på profilering, konsekvenserna av sådan behandling. Om möjligt bör den personuppgiftsansvarige kunna ge fjärråtkomst till ett säkert system genom vilket den registrerade kan få direkt åtkomst till sina personuppgifter. Denna rätt bör inte inverka menligt på andras rättigheter eller friheter, t.ex. affärshemligheter eller immateriell äganderätt och särskilt inte på upphovsrätt som skyddar programvaran. Resultatet av dessa överväganden bör dock inte bli att den registrerade förvägras all information. Om den personuppgiftsansvarige behandlar en stor mängd uppgifter om den registrerade, bör den personuppgiftsansvarige kunna begära att den registrerade lämnar uppgift om vilken information eller vilken behandling en framställan avser, innan informationen lämnas ut.
- (64) Personuppgiftsansvariga bör vidta alla rimliga åtgärder för att kontrollera identiteten på en registrerad som begär tillgång, särskilt inom ramen för nättjänster och i fråga om nätidentifierare. Personuppgiftsansvariga bör inte behålla personuppgifter enbart för att kunna agera vid en potentiell begäran.
- (65) Den registrerade bör ha rätt att få sina personuppgifter rättade och en rätt att bli bortglömd, om lagringen av uppgifterna strider mot denna förordning eller unionsrätten eller medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av. En registrerad bör särskilt ha rätt att få sina personuppgifter raderade och kunna begära att dessa personuppgifter inte behandlas, om de inte längre behövs med tanke på de ändamål för vilka de samlats in eller på annat sätt behandlats, om en registrerad har återtagit sitt samtycke till behandling eller invänder mot behandling av personuppgifter som rör honom eller henne, eller om behandlingen av hans eller

hennes personuppgifter på annat sätt inte överensstämmer med denna förordning. Denna rättighet är särskilt relevant när den registrerade har gett sitt samtycke som barn, utan att vara fullständigt medveten om riskerna med behandlingen, och senare vill ta bort dessa personuppgifter, särskilt på internet. Den registrerade bör kunna utöva denna rätt även när han eller hon inte längre är barn. Ytterligare lagring av personuppgifterna bör dock vara laglig, om detta krävs för att utöva yttrandefrihet och informationsfrihet, för att uppfylla en rättslig förpliktelse, för att utföra en uppgift i av allmänt intresse eller som ett led i myndighetsutövning som anförtrots den personuppgiftsansvarige, med anledning av ett allmänt intresse inom folkhälsoområdet, för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål eller för fastställande, utövande eller försvar av rättsliga anspråk.

- (66) För att stärka "rätten att bli bortglömd" i nätmiljön bör rätten till radering utvidgas genom att personuppgiftsansvariga som offentliggjort personuppgifter är förpliktigade att vidta rimliga åtgärder, däribland tekniska åtgärder, för att informera de personuppgiftsansvariga som behandlar dessa personuppgifter om att den registrerade har begärt radering av alla länkar till och kopior eller reproduktioner av dessa personuppgifter. I samband med detta bör den personuppgiftsansvarige vidta rimliga åtgärder, med beaktande av tillgänglig teknik och de hjälpmedel som står den personuppgiftsansvarige till buds, däribland tekniska åtgärder, för att informera de personuppgiftsansvariga som behandlar personuppgifterna om den registrerades begäran.
- (67) Sätten att begränsa behandlingen av personuppgifter kan bland annat innebära att man tillfälligt flyttar de valda personuppgifterna till ett annat databehandlingssystem, gör de valda uppgifterna otillgängliga för användare eller tillfälligt avlägsnar offentliggjorda uppgifter från en webbplats. I automatiserade register bör begränsningen av behandlingen i princip ske med tekniska medel på ett sådant sätt att personuppgifterna inte blir föremål för ytterligare behandling och inte kan ändras. Det förhållande att behandlingen av personuppgifter är begränsad bör klart anges inom systemet.
- (68) För att ytterligare förbättra kontrollen över sina egna uppgifter bör den registrerade, om personuppgifterna behandlas automatiskt, också tillåtas att motta de personuppgifter som rör honom eller henne, som han eller hon har tillhandahållit den personuppgiftsansvarige, i ett strukturerat, allmänt använt, maskinläsbart och kompatibelt format och överföra dessa till en annan personuppgiftsansvarig. Personuppgiftsansvariga bör uppmuntras att utveckla kompatibla format som möjliggör dataportabilitet. Denna rättighet bör vara tillämplig om den registrerade har tillhandahållit uppgifterna efter att ha lämnat sitt samtycke eller om behandlingen är nödvändig för att ett avtal ska kunna genomföras. Den bör inte vara tillämplig om behandlingen utgår från en annan rättslig grund än samtycke eller avtal. På grund av sin art bör denna rättighet inte utövas mot personuppgiftsansvariga som behandlar personuppgifter som ett led i myndighetsutövning. Därför bör den inte vara tillämplig när behandlingen av personuppgifterna är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning som utförs av den personuppgiftsansvarige. Den registrerades rätt att överföra eller motta personuppgifter som rör honom eller henne innebär inte någon skyldighet för de personuppgiftsansvariga att införa eller upprätthålla behandlingssystem som är tekniskt kompatibla. Om mer än en registrerad berörs inom en viss uppsättning personuppgifter, bör rätten att motta personuppgifterna inte inverka på andra registrerades rättigheter och friheter enligt denna förordning. Denna rättighet bör inte heller påverka den registrerades rätt att få till stånd radering av personuppgifter och de inskränkningar av denna rättighet vilka anges i denna förordning och bör i synnerhet inte medföra radering av personuppgifter om den registrerade som denne har lämnat för genomförande av ett avtal, i den utsträckning och så länge som personuppgifterna krävs för genomförande av avtalet. Om det är tekniskt möjligt, bör den registrerade ha rätt till direkt överföring av personuppgifterna från en personuppgiftsansvarig till en annan.
- (69) När personuppgifter lagligen får behandlas, eftersom behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i en myndighetsutövning som utförs av den personuppgiftsansvarige, eller på grund av en personuppgiftsansvarigs eller en tredje parts berättigade intressen, bör alla registrerade ändå ha rätt att göra invändningar mot behandling av personuppgifter som rör de registrerades särskilda situation. Det bör ankomma på den personuppgiftsansvarige att visa att dennes tvingande berättigade intressen väger tyngre än den registrerades intressen eller grundläggande rättigheter och friheter.
- (70) Om personuppgifter behandlas för direktmarknadsföring, bör den registrerade, oavsett om det handlar om inledande eller ytterligare behandling, ha rätt att när som helst kostnadsfritt invända mot sådan behandling, inbegripet profilering, i den mån denna är kopplad till direktmarknadsföring. Denna rättighet bör uttryckligen meddelas den registrerade och redovisas tydligt, klart och åtskilt från annan information.

- (71) Den registrerade bör ha rätt att inte bli föremål för ett beslut, vilket kan innebära en åtgärd, med bedömning av personliga aspekter rörande honom eller henne, vilket enbart grundas på automatiserad behandling och medför rättsverkan för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne, såsom ett automatiserat avslag på en kreditansökan online eller e-rekrytering utan personlig kontakt. Sådan behandling omfattar "profilering" i form av automatisk behandling av personuppgifter med bedömning av personliga aspekter rörande en fysisk person, särskilt för att analysera eller förutse aspekter avseende den registrerades arbetsprestation, ekonomiska situation, hälsa, personliga preferenser eller intressen, pålitlighet eller beteende, vistelseort eller förflyttningar, i den mån dessa har rättsverkan rörande honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne. Beslutsfattande grundat på sådan behandling, inbegripet profilering, bör dock tillåtas när det uttryckligen beviljas genom unionsrätten eller medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av, inbegripet för sådan övervakning och sådant förebyggande av bedrägerier och skatteundandragande som genomförs i enlighet med unionsinstitutionernas eller de nationella tillsynsorganens bestämmelser, standarder och rekommendationer samt för att sörja för tillförlitlighet hos en tjänst som tillhandahålls av den personuppgiftsansvarige, eller när det krävs för ingående eller genomförande av ett avtal mellan den registrerade och en personuppgiftsansvarig eller den registrerade har gett sitt uttryckliga samtycke. Denna form av uppgiftsbehandling bör under alla omständigheter omgärdas av lämpliga skyddsåtgärder, som bör inkludera specifik information till den registrerade och rätt till mänskligt ingripande, att framföra sina synpunkter, att erhålla en förklaring till det beslut som fattas efter sådan bedömning och att överklaga beslutet. Sådana åtgärder bör inte gälla barn.

I syfte att sörja för rättvis och transparent behandling med avseende på den registrerade, med beaktande av omständigheterna och det sammanhang i vilket personuppgifterna behandlas, bör den personuppgiftsansvarige använda adekvata matematiska eller statistiska förfaranden för profilering, genomföra tekniska och organisatoriska åtgärder som framför allt säkerställer att faktorer som kan medföra felaktigheter i personuppgifter korrigeras och att risken för fel minimeras samt säkra personuppgifterna på sådant sätt att man beaktar potentiella risker för den registrerades intressen och rättigheter och förhindrar bland annat diskriminerande effekter för fysiska personer, på grund av ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse, medlemskap i fackföreningar, genetisk status eller hälsostatus eller sexuell läggning, eller som leder till åtgärder som får sådana effekter. Automatiserat beslutsfattande och profilering baserat på särskilda kategorier av personuppgifter bör endast tillåtas på särskilda villkor.

- (72) Profilering omfattas av denna förordnings bestämmelser om behandling av personuppgifter, såsom de rättsliga grunderna för behandlingen och principer för dataskydd. Europeiska dataskyddsstyrelsen som inrättas genom denna förordning (nedan kallad *styrelsen*) bör kunna utfärda riktlinjer i detta avseende.
- (73) Begränsningar med avseende på specifika principer och rätten till information, tillgång till och rättelse eller radering av personuppgifter, rätten till dataportabilitet, rätten att göra invändningar, profileringsbaserade beslut samt information till den registrerade om personuppgiftsincidenter och vissa av den personuppgiftsansvariges relaterade skyldigheter kan införas genom unionsrätten eller medlemsstaternas nationella rätt, i den mån de är nödvändiga och proportionella i ett demokratiskt samhälle för att upprätthålla den allmänna säkerheten, exempelvis för att skydda människoliv, särskilt vid naturkatastrofer eller katastrofer framkallade av människan, vid förebyggande, förhindrande, utredning och lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten eller överträdelser av etiska principer för reglerade yrken, vad gäller unionens eller en medlemsstats övriga viktiga mål av allmänt intresse, särskilt om de är av stort ekonomiskt eller finansiellt intresse för unionen eller en medlemsstat, förande av offentliga register som förs av hänsyn till ett allmänt intresse, ytterligare behandling av arkiverade personuppgifter för att tillhandahålla specifik information om politiskt beteende under tidigare totalitära regimer eller skydd av den registrerade eller andras rättigheter och friheter, inklusive socialt skydd, folkhälsa och humanitära skäl. Dessa begränsningar bör överensstämma med kraven i stadgan och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.
- (74) Personuppgiftsansvariga bör åläggas ansvaret för all behandling av personuppgifter som de utför eller som utförs på deras vägnar. Personuppgiftsansvariga bör särskilt vara skyldiga att vidta lämpliga och effektiva åtgärder och kunna visa att behandlingen är förenlig med denna förordning, även vad gäller åtgärdernas effektivitet. Man bör inom dessa åtgärder beakta behandlingens art, omfattning, sammanhang och ändamål samt risken för fysiska personers rättigheter och friheter.

- (75) Risken för fysiska personers rättigheter och friheter, av varierande sannolikhetsgrad och allvar, kan uppkomma till följd av personuppgiftsbehandling som skulle kunna medföra fysiska, materiella eller immateriella skador, i synnerhet om behandlingen kan leda till diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, obehörigt hävande av pseudonymisering eller annan betydande ekonomisk eller social nackdel, om registrerade kan berövas sina rättigheter och friheter eller hindras att utöva kontroll över sina personuppgifter, om personuppgifter behandlas som avslöjar ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse eller medlemskap i fackförening, om genetiska uppgifter, uppgifter om hälsa eller sexualliv eller fällande domar i brottmål samt överträdelse eller därmed sammanhängande säkerhetsåtgärder behandlas, om personliga aspekter bedöms, framför allt analyser eller förutsägelser beträffande sådant som rör arbetsprestationer, ekonomisk ställning, hälsa, personliga preferenser eller intressen, tillförlitlighet eller beteende, vistelseort eller förflyttningar, i syfte att skapa eller använda personliga profiler, om det sker behandling av personuppgifter rörande sårbara fysiska personer, framför allt barn, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.
- (76) Hur sannolik och allvarlig risken för den registrerades rättigheter och friheter är bör fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål. Risken bör utvärderas på grundval av en objektiv bedömning, genom vilken det fastställs huruvida uppgiftsbehandlingen inbegriper en risk eller en hög risk.
- (77) Vägledning för den personuppgiftsansvariges eller personuppgiftsbitrådets genomförande av lämpliga åtgärder och för påvisande av att behandlingen är förenlig med denna förordning, särskilt när det gäller att kartlägga den risk som är förknippad med behandlingen och bedöma dess ursprung, art, sannolikhetsgrad och allvar samt fastställa bästa praxis för att minska risken, kan framför allt ges genom godkända uppförandekoder, godkänd certifiering, riktlinjer från styrelsen eller genom anvisningar från ett dataskyddsbud. Styrelsen kan också utfärda riktlinjer för uppgiftsbehandling som inte bedöms medföra någon hög risk för fysiska personers rättigheter och friheter samt ange vilka åtgärder som i sådana fall kan vara tillräckliga för att bemöta en sådan risk.
- (78) Skyddet av fysiska personers rättigheter och friheter i samband med behandling av personuppgifter förutsätter att lämpliga tekniska och organisatoriska åtgärder vidtas, så att kraven i denna förordning uppfylls. För att kunna visa att denna förordning följs bör den personuppgiftsansvarige anta interna strategier och vidta åtgärder, särskilt för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard. Sådana åtgärder kan bland annat bestå av att uppgiftsbehandlingen minimeras, att personuppgifter snarast möjligt pseudonymiseras, att öppenhet om personuppgifternas syfte och behandling iakttas, att den registrerade får möjlighet att övervaka uppgiftsbehandlingen och att den personuppgiftsansvarige får möjlighet att skapa och förbättra säkerhetsanordningar. Vid utveckling, utformning, urval och användning av applikationer, tjänster och produkter som är baserade på behandling av personuppgifter eller behandlar personuppgifter för att uppfylla sitt syfte bör producenterna av dessa produkter, tjänster och applikationer uppmanas att beakta rätten till dataskydd när sådana produkter, tjänster och applikationer utvecklas och utformas och att, med tillbörlig hänsyn till den tekniska utvecklingen, säkerställa att personuppgiftsansvariga och personuppgiftsbitråden kan fullgöra sina skyldigheter avseende dataskydd. Principerna om inbyggt dataskydd och dataskydd som standard bör också beaktas vid offentliga upphandlingar.
- (79) Skyddet av de registrerades rättigheter och friheter samt de personuppgiftsansvarigas och personuppgiftsbitrådenas ansvar, även i förhållande till tillsynsmyndigheternas övervakning och åtgärder, kräver ett tydligt fastställande av vem som bär ansvaret enligt denna förordning, bl.a. när personuppgiftsansvariga gemensamt fastställer ändamål och medel för en behandling tillsammans med andra personuppgiftsansvariga eller när en behandling utförs på en personuppgiftsansvarigs vägnar.
- (80) När personuppgiftsansvariga eller personuppgiftsbitråden som inte är etablerade inom unionen behandlar personuppgifter om registrerade som befinner sig inom unionen och det bakomliggande syftet med uppgiftsbehandlingen är att erbjuda de registrerade personerna i unionen varor eller tjänster, oberoende av om de registrerade personerna måste betala för dem, eller att övervaka deras beteende i den mån beteendet äger rum i unionen, bör de personuppgiftsansvariga eller personuppgiftsbitrådena utnämna en företrädare, såvida inte behandlingen endast är tillfällig, inte omfattar behandling i stora kategorier av särskilda kategorier av personuppgifter eller behandling av personuppgifter om fällande domar i brottmål samt överträdelse och det är

osannolikt att den inbegriper en risk för fysiska personers rättigheter och friheter, med beaktande av behandlingens art, sammanhang, omfattning och ändamål eller om den personuppgiftsansvarige är en myndighet eller ett organ. Företrädaren bör agera på den personuppgiftsansvariges eller på personuppgiftsbitrådets vägnar och kan kontaktas av samtliga tillsynsmyndigheter. Företrädaren bör uttryckligen utses genom en skriftlig fullmakt från den personuppgiftsansvarige eller från personuppgiftsbitrådet att agera på dennes vägnar med avseende på dennes skyldigheter enligt denna förordning. Utnämningen av företrädaren inverkar inte på den personuppgiftsansvariges eller på personuppgiftsbitrådets ansvar enligt denna förordning. Företrädaren bör utföra sina uppgifter i enlighet med erhållen fullmakt från den personuppgiftsansvarige eller från personuppgiftsbitrådet, vilket inbegriper samarbete med de behöriga tillsynsmyndigheterna i fråga om alla åtgärder som vidtas för att sörja för efterlevnad av denna förordning. Den utsedda företrädaren bör underkastas verkställighetsförfaranden i händelse den personuppgiftsansvarige eller personuppgiftsbitrådet inte uppfyller sina skyldigheter.

- (81) För att se till att kraven i denna förordning uppfylls vad gäller behandling som av ett personuppgiftsbiträde ska utföras på en personuppgiftsansvarigs vägnar ska den personuppgiftsansvarige, när denne anförtror behandling åt ett personuppgiftsbiträde, endast använda personuppgiftsbitråden som ger tillräckliga garantier, i synnerhet i fråga om sakkunskap, tillförlitlighet och resurser, för att genomföra tekniska och organisatoriska åtgärder som uppfyller kraven i denna förordning, bl.a. vad gäller säkerhet i samband med behandlingen av uppgifter. Personuppgiftsbitrådets anslutning till en godkänd uppförandekod eller en godkänd certifieringsmekanism kan användas som ett sätt att påvisa att den personuppgiftsansvarige fullgör sina skyldigheter. När uppgifter behandlas av ett personuppgiftsbiträde, bör hanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller medlemsstaternas nationella rätt mellan personuppgiftsbitrådet och den personuppgiftsansvarige, där föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade anges, med beaktande av personuppgiftsbitrådets specifika arbets- och ansvarsuppgifter inom ramen för den behandling som ska utföras och risken med avseende på den registrerades rättigheter och friheter. Den personuppgiftsansvarige och personuppgiftsbitrådet får välja att använda sig av ett enskilt avtal eller standardavtalsklausuler som antingen antas direkt av kommissionen eller av en tillsynsmyndighet i enlighet med mekanismen för enhetlighet och därefter antas av kommissionen. Efter det att behandlingen på den personuppgiftsansvariges vägnar har avslutats, bör personuppgiftsbitrådet återlämna eller radera personuppgifterna, beroende på vad den personuppgiftsansvarige väljer, såvida inte lagring av personuppgifterna krävs enligt den unionsrätt eller medlemsstaternas nationella rätt som personuppgiftsbitrådet omfattas av.
- (82) För att påvisa att denna förordning följs bör de personuppgiftsansvariga eller personuppgiftsbitrådena föra register över behandling som sker under deras ansvar. Alla personuppgiftsansvariga och personuppgiftsbitråden bör vara skyldiga att samarbeta med tillsynsmyndigheten och på dennas begäran göra detta register tillgängligt, så att det kan tjäna som grund för övervakningen av behandlingen.
- (83) För att upprätthålla säkerheten och förhindra behandling som bryter mot denna förordning bör personuppgiftsansvariga eller personuppgiftsbitråden utvärdera riskerna med behandlingen och vidta åtgärder, såsom kryptering, för att minska dem. Åtgärderna bör säkerställa en lämplig säkerhetsnivå, inbegripet konfidentialitet, med beaktande av den senaste utvecklingen och genomförandekostnader i förhållande till riskerna och vilken typ av personuppgifter som ska skyddas. Vid bedömningen av datasäkerhetsrisken bör man även beakta de risker som personuppgiftsbehandling medför, såsom förstöring, förlust eller ändringar genom olyckshändelse eller otillåtna handlingar eller obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats, framför allt när denna kan medföra fysisk, materiell eller immateriell skada.
- (84) I syfte att sörja för bättre efterlevnad av denna förordning när behandlingen sannolikt kan innebära en hög risk för fysiska personers rättigheter och friheter, bör den personuppgiftsansvarige vara ansvarig för att en konsekvensbedömning utförs avseende dataskydd för att bedöma framför allt riskens ursprung, art, särdrag och allvar. Resultatet av denna bedömning bör beaktas vid fastställandet av de lämpliga åtgärder som ska vidtas för att visa att behandlingen av personuppgifter är förenlig med denna förordning. I de fall en konsekvensbedömning avseende dataskydd ger vid handen att uppgiftsbehandlingen medför en hög risk, som den personuppgiftsansvarige inte kan begränsa genom lämpliga åtgärder med avseende på tillgänglig teknik och genomförandekostnader, bör ett samråd med tillsynsmyndigheten ske före behandlingen.
- (85) En personuppgiftsincident som inte snabbt åtgärdas på lämpligt sätt kan för fysiska personer leda till fysisk, materiell eller immateriell skada, såsom förlust av kontrollen över de egna personuppgifterna eller till begränsning av deras rättigheter, diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, obehörigt hävande av pseudonymisering, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, eller till annan ekonomisk eller social nackdel för den berörda fysiska personen. Så

snart en personuppgiftsansvarig blir medveten om att en personuppgiftsincident har inträffat, bör den personuppgiftsansvarige därför anmäla personuppgiftsincidenten till tillsynsmyndigheten utan onödigt dröjsmål och, om så är möjligt, inom 72 timmar efter att ha blivit medveten om denna, om inte den personuppgiftsansvarige, i enlighet med ansvarsprincipen, kan påvisa att det är osannolikt att personuppgiftsincidenten kommer att medföra en risk för fysiska personers rättigheter och friheter. Om en sådan anmälan inte kan ske inom 72 timmar, bör skälen till fördröjningen åtfölja anmälan och information får lämnas i omgångar utan otillbörligt vidare dröjsmål.

- (86) Den personuppgiftsansvarige bör utan onödigt dröjsmål underrätta den registrerade om en personuppgiftsincident, om personuppgiftsincidenten sannolikt kommer att medföra en hög risk för den fysiska personens rättigheter och friheter, så att denne kan vidta nödvändiga försiktighetsåtgärder. Denna underrättelse bör beskriva personuppgiftsincidentens art samt innehålla rekommendationer för den berörda fysiska personen om hur de potentiella negativa effekterna kan mildras. De registrerade bör underrättas så snart detta rimligtvis är möjligt, i nära samarbete med tillsynsmyndigheten och i enlighet med den vägledning som lämnats av den eller andra relevanta myndigheter, exempelvis brottsbekämpande myndigheter. Till exempel kräver behovet av att mildra en omedelbar skaderisk att de registrerade underrättas omedelbart, medan behovet av att vidta lämpliga åtgärder vid fortlopande eller likartade personuppgiftsincidenter däremot kan motivera längre tid för underrättelsen.
- (87) Det bör undersökas huruvida alla lämpliga tekniska skyddsåtgärder och alla lämpliga organisatoriska åtgärder har vidtagits för att omedelbart fastställa om en personuppgiftsincident har ägt rum och skyndsamt informera tillsynsmyndigheten och den registrerade. Att en anmälan gjordes utan onödigt dröjsmål bör fastställas med hänsyn tagen bl.a. till personuppgiftsincidentens art och svårighetsgrad och dess följder och negativa effekter för den registrerade. En sådan anmälan kan leda till ett ingripande från tillsynsmyndighetens sida i enlighet med dess uppgifter och befogenheter enligt denna förordning.
- (88) När ingående regler fastställs för format och förfaranden för anmälan av personuppgiftsincidenter, bör vederbörlig hänsyn tas till omständigheterna kring incidenten, däribland om personuppgifterna var skyddade av lämpliga tekniska skyddsåtgärder, som betydligt begränsar sannolikheten för identitetsbedrägeri eller andra former av missbruk. Dessutom bör sådana regler och förfaranden beakta brottsbekämpande myndigheters berättigade intressen, där en för tidig redovisning kan riskera att i onödan hämma utredning av omständigheterna kring en personuppgiftsincident.
- (89) Direktiv 95/46/EG föreskrev en allmän skyldighet att anmäla behandling av personuppgifter till tillsynsmyndigheterna. Denna skyldighet medförde administrativa och ekonomiska bördor, men förbättrade inte alltid personuppgiftsskyddet. Sådana övergripande och allmänna anmälningsskyldigheter bör därför avskaffas och ersättas av effektiva förfaranden och mekanismer som i stället inriktas på de typer av behandlingar som sannolikt innebär en hög risk för fysiska personers rättigheter och friheter, i kraft av deras art, omfattning, sammanhang och ändamål. Dessa behandlingar kan vara sådana som särskilt inbegriper användning av ny teknik eller är av en ny typ, för vilken konsekvensbedömning avseende uppgiftsskydd inte tidigare har genomförts av den personuppgiftsansvarige, eller som blir nödvändiga på grund av den tid som har förflutit sedan den ursprungliga behandlingen.
- (90) I sådana fall bör den personuppgiftsansvarige före behandlingen, med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt upphovet till risken, göra en konsekvensbedömning avseende dataskydd i syfte att bedöma den höga riskens specifika sannolikhetsgrad och allvar samt dess ursprung. Konsekvensbedömningen bör främst innefatta de planerade åtgärder, skyddsåtgärder och mekanismer som ska minska denna risk, säkerställa personuppgiftsskyddet och visa att denna förordning efterlevs.
- (91) Detta bör särskilt vara tillämpligt på storskalig uppgiftsbehandling med syftet att behandla betydande mängder personuppgifter på regional, nationell eller övernationell nivå, vilket skulle kunna påverka ett stort antal registrerade och sannolikt kommer att innebära en hög risk, exempelvis till följd av uppgifternas känsliga natur, där i enlighet med den uppnådda nivån av teknisk kunskap en ny teknik används storskaligt, samt på annan behandling som innebär en hög risk för registrerades rättigheter och friheter, framför allt när denna behandling gör det svårare för de registrerade att utöva sina rättigheter. En konsekvensbedömning avseende dataskydd bör

också göras, där personuppgifter behandlas i syfte att fatta beslut om specifika fysiska personer efter en systematisk och omfattande bedömning av fysiska personers personliga aspekter på grundval av profilering av dessa uppgifter eller efter behandling av särskilda kategorier av personuppgifter, biometriska uppgifter eller uppgifter om fällande domar i brottmål samt överträdelser eller därmed sammanhängande säkerhetsåtgärder. Likaså krävs en konsekvensbedömning avseende dataskydd för övervakning av allmän plats i stor omfattning, särskilt vid användning av optisk-elektroniska anordningar, eller för all annan behandling där den behöriga tillsynsmyndigheten anser att behandlingen sannolikt kommer att innebära en hög risk för de registrerades rättigheter och friheter, framför allt på grund av att den hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal eller på grund av att den systematiskt genomförs i stor omfattning. Behandling av personuppgifter bör inte anses vara storskalig, om det är fråga om personuppgifter från patienter eller klienter som behandlas av enskilda läkare, andra yrkesverksamma på hälsoområdet eller juridiska ombud. I dessa fall bör en konsekvensbedömning avseende dataskydd inte vara obligatorisk.

- (92) Ibland kan det vara förnuftigt och ekonomiskt att en konsekvensbedömning avseende dataskydd inriktar sig på ett vidare område än ett enda projekt, exempelvis när myndigheter eller organ avser att skapa en gemensam tillämpnings- eller behandlingsplattform eller när flera personuppgiftsansvariga planerar att införa en gemensam tillämpnings- eller behandlingsmiljö för en hel bransch eller ett helt segment eller för en allmänt utnyttjad horisontell verksamhet.
- (93) Medlemsstaterna kan anse det nödvändigt att genomföra en sådan bedömning före behandlingen i samband med antagandet av medlemsstaters nationella rätt som ligger till grund för utförandet av myndighetens eller det offentliga organets uppgifter och reglerar den aktuella specifika behandlingsåtgärden eller serien av åtgärder.
- (94) Om det av en konsekvensbedömning avseende dataskydd framgår att behandlingen utan skyddsåtgärder, säkerhetsåtgärder och mekanismer för att minska risken kommer att innebära en hög risk för fysiska personers rättigheter och friheter, och den personuppgiftsansvarige anser att risken inte kan begränsas genom åtgärder som är rimliga med avseende på tillgänglig teknik och genomförandekostnader, bör samråd hållas med tillsynsmyndigheten innan behandlingen inleds. En sådan hög risk kommer sannolikt att orsakas av vissa typer av behandling samt av en viss omfattning och frekvens för behandlingen, vilket även kan leda till skador för eller kränkningar av fysiska personers rättigheter och friheter. Tillsynsmyndigheten bör inom en fastställd tid svara på en begäran om samråd. Ett uteblivet svar från tillsynsmyndigheten inom denna tid bör dock inte hindra ett eventuellt ingripande från tillsynsmyndighetens sida i enlighet med dess uppgifter och befogenheter enligt denna förordning, inbegripet befogenheten att förbjuda behandling. Som en del av denna samrådsprocess får resultatet av en konsekvensbedömning avseende dataskydd som utförs med avseende på behandlingen i fråga överlämnas till tillsynsmyndigheten, framför allt de åtgärder som planeras för att minska risken för fysiska personers rättigheter och friheter.
- (95) Personuppgiftsbiträdet bör vid behov och på begäran bistå den personuppgiftsansvarige med fullgörande av de skyldigheter som härrör från utförandet av konsekvensbedömningar avseende dataskydd och förhandssamråd med tillsynsmyndigheten.
- (96) Ett samråd med tillsynsmyndigheten bör även ske som ett led i det förberedande arbetet med en lagstiftningsåtgärd som stadgar om behandling av personuppgifter i syfte att säkerställa att den avsedda behandlingen överensstämmer med denna förordning och framför allt för att minska den risk den medför för den registrerade.
- (97) När en behandling utförs av en myndighet, med undantag av domstolar eller oberoende rättsliga myndigheter som en del av deras dömande verksamhet, eller när en behandling utförs i den privata sektorn av en personuppgiftsansvarig vars kärnverksamhet består av behandlingsverksamhet som kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning, eller när den personuppgiftsansvariges eller personuppgiftsbitrådets kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av personuppgifter och uppgifter som rör fällande domar i brottmål och överträdelser, bör en person med sakkunskap i fråga om dataskyddslagstiftning och -förfaranden bistå den personuppgiftsansvarige eller personuppgiftsbiträdet för att övervaka den interna efterlevnaden av denna förordning. I den privata sektorn avser personuppgiftsansvarigas kärnverksamhet deras primära verksamhet och inte behandling av personuppgifter som kompletterande verksamhet. Den nödvändiga nivån på sakkunskapen bör fastställas särskilt i enlighet med den uppgiftsbehandling

som utförs och det skydd som krävs för de personuppgifter som behandlas av den personuppgiftsansvarige eller personuppgiftsbiträdet. Denna typ av dataskyddsbud bör, oavsett om de är anställda av den personuppgiftsansvarige eller ej, kunna fullgöra sitt uppdrag och utföra sina uppgifter på ett oberoende sätt.

- (98) Sammanslutningar eller andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden bör uppmanas att utarbeta uppförandekoder inom gränserna för denna förordning, så att tillämpningen av denna förordning effektiviseras, med beaktande av särdragen hos den behandling som sker inom vissa sektorer och de särskilda behov som finns inom mikroföretag samt inom små och medelstora företag. I synnerhet skulle man genom sådana uppförandekoder kunna anpassa personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter, med beaktande av den risk som behandlingen sannolikt innebär för fysiska personers rättigheter och friheter.
- (99) Vid utformningen av en uppförandekod eller vid ändring eller utvidgning av en befintlig sådan kod bör sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden samråda med berörda intressenter, i möjligaste mån inbegripet registrerade, och beakta de inlagor som mottas och de åsikter som framförs som svar på samråden.
- (100) För att förbättra öppenheten och efterlevnaden av denna förordning bör införandet av certifieringsmekanismer och dataskyddsförsegling och dataskyddsmärkning uppmanas, så att registrerade snabbt kan bedöma nivån på relevanta produkters och tjänsters dataskydd.
- (101) Flöden av personuppgifter till och från länder utanför unionen och till och från internationella organisationer är nödvändiga för utvecklingen av internationell handel och internationellt samarbete. Ökningen av dessa flöden har medfört nya utmaningar och nya farhågor när det gäller skyddet av personuppgifter. Det är viktigt att den skyddsnivå som fysiska personer säkerställs inom unionen genom denna förordning inte undergrävs när personuppgifter överförs från unionen till personuppgiftsansvariga, personuppgiftsbiträden eller andra mottagare i tredjeland eller till internationella organisationer, vilket inbegriper vidarebefordran av personuppgifter från tredjelandet eller den internationella organisationen till personuppgiftsansvariga, personuppgiftsbiträden i samma eller ett annat tredjeland eller en annan internationell organisation. Överföringar till tredjeländer och internationella organisationer får under alla omständigheter endast utföras i full överensstämmelse med denna förordning. En överföring kan endast ske, om de villkor som fastställs i bestämmelserna i denna förordning om överföring av personuppgifter till tredjeländer eller internationella organisationer har uppfyllts av den personuppgiftsansvarige eller personuppgiftsbiträdet, med förbehåll för de övriga bestämmelserna i denna förordning.
- (102) Denna förordning påverkar inte internationella avtal mellan unionen och tredjeländer som reglerar överföring av personuppgifter, däribland lämpliga skyddsåtgärder för de registrerade. Medlemsstaterna får ingå internationella avtal som innefattar överföring av personuppgifter till tredjeländer eller internationella organisationer i den mån sådana avtal inte påverkar denna förordning eller andra bestämmelser i unionsrätten och innehåller en skälig nivå av skydd för de registrerades grundläggande rättigheter.
- (103) Kommissionen kan med verkan för hela unionen fastställa att ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland eller en internationell organisation erbjuder en adekvat dataskyddsnivå och på så sätt skapa rättslig säkerhet och enhetlighet i hela unionen vad gäller tredjelandet eller den internationella organisationen som anses tillhandahålla en sådan skyddsnivå. I dessa fall får överföringar av personuppgifter till det tredjelandet eller den internationella organisationen ske utan ytterligare tillstånd. Kommissionen kan också, efter att ha underrättat tredjelandet eller den internationella organisationen och lämnat en fullständig motivering, besluta att ett sådant beslut ska återkallas.
- (104) I enlighet med de grundläggande värderingar som unionen bygger på, bl.a. skyddet av mänskliga rättigheter, bör kommissionen i sin bedömning av tredjelandet eller ett territorium eller en specificerad sektor i ett tredjeland beakta hur ett visst tredjeland respekterar rättsstatsprincipen, tillgången till rättslig prövning samt internationella människorättsnormer och -standarder samt landets allmänna lagstiftning och sektorslagstiftning, inklusive lagstiftning om allmän säkerhet, försvar och nationell säkerhet samt allmän ordning och straffrätt. Vid antagandet av ett beslut om adekvat skyddsnivå avseende ett territorium eller en specificerad sektor i ett tredjeland bör hänsyn tas till tydliga och objektiva kriterier, t.ex. specifik behandling och tillämpningsområdet för tillämpliga rättsliga standarder och gällande lagstiftning i tredjelandet. Tredjelandet bör erbjuda garantier som säkerställer en

tillfredsställande skyddsnivå som i huvudsak motsvarar den som säkerställs i unionen, i synnerhet när personuppgifter behandlas inom en eller flera specifika sektorer. Tredjelandet bör framför allt säkerställa en effektiv oberoende dataskyddsövervakning och sörja för samarbetsmekanismer med medlemsstaternas dataskyddsmyndigheter, och de registrerade bör tillförsäkras effektiva och lagstadgade rättigheter samt effektiv administrativ och rättslig prövning.

- (105) Utöver de internationella åtaganden som tredjelandet eller den internationella organisationen har gjort bör kommissionen beakta de skyldigheter som följer av tredjelandets eller den internationella organisationens deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter och genomförandet av dessa skyldigheter. Framför allt bör tredjelandets anslutning till Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk behandling av personuppgifter och dess tilläggsprotokoll beaktas. Kommissionen bör samråda med styrelsen vid bedömningen av skyddsnivån i tredjeländer eller internationella organisationer.
- (106) Kommissionen bör övervaka hur beslut om skyddsnivå i ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland eller en internationell organisation fungerar, och övervaka hur beslut som antas på grundval av artikel 25.6 eller 26.4 i direktiv 95/46/EG fungerar. Kommissionen bör i sina beslut om adekvat skyddsnivå föreskriva en mekanism för periodisk översyn av hur de fungerar. Denna periodiska översyn bör genomföras i samråd med det berörda tredjelandet eller den berörda internationella organisationen, med beaktande av all relevant utveckling i tredjelandet eller den internationella organisationen. Vid övervakningen och genomförandet av den periodiska översynen bör kommissionen ta hänsyn till synpunkter och resultat från Europaparlamentet och rådet samt andra relevanta organ och källor. Kommissionen bör inom rimlig tid utvärdera hur de sistnämnda besluten fungerar och rapportera alla relevanta resultat till den kommitté, i den mening som avses i Europaparlamentets och rådets förordning (EU) nr 182/2011 ⁽¹⁾, som inrättats enligt denna förordning och till Europaparlamentet och rådet.
- (107) Kommissionen kan konstatera att ett tredjeland, ett territorium eller en viss specificerad sektor i ett tredjeland eller en internationell organisation inte längre säkerställer en adekvat dataskyddsnivå. Överföring av personuppgifter till detta tredjeland eller till denna internationella organisation bör då förbjudas, såvida inte kraven i denna förordning avseende överföring med stöd av lämpliga skyddsåtgärder, inbegripet bindande företagsbestämmelser och undantag för särskilda situationer, är uppfyllda. I så fall bör det finnas möjlighet till samråd mellan kommissionen och dessa tredjeländer eller internationella organisationer. Kommissionen bör i god tid informera tredjelandet eller den internationella organisationen om skälen och inleda samråd med tredjelandet eller organisationen för att avhjälpa situationen.
- (108) Saknas beslut om adekvat skyddsnivå bör den personuppgiftsansvarige eller personuppgiftsbiträdet vidta åtgärder för att kompensera för det bristande dataskyddet i ett tredjeland med hjälp av lämpliga skyddsåtgärder för den registrerade. Sådana lämpliga skyddsåtgärder kan bestå i tillämpning av bindande företagsbestämmelser, standardbestämmelser om dataskydd som antagits av kommissionen, standardbestämmelser om dataskydd som antagits av en tillsynsmyndighet eller avtalsbestämmelser som godkänts av en tillsynsmyndighet. Dessa skyddsåtgärder bör säkerställa iakttagande av de krav i fråga om dataskydd och registrerades rättigheter som är lämpliga för behandling inom unionen, inbegripet huruvida bindande rättigheter för de registrerade och effektiva rättsmedel är tillgängliga, inbegripet en faktisk rätt att föra talan på administrativ väg eller inför domstol och att kräva kompensation i unionen eller i ett tredjeland. De bör särskilt gälla överensstämmelse med allmänna principer för behandling av personuppgifter samt principerna om inbyggt dataskydd och dataskydd som standard. Överföring av uppgifter kan också utföras av offentliga myndigheter eller organ till offentliga myndigheter eller organ i tredjeländer eller internationella organisationer med motsvarande skyldigheter eller uppgifter, inbegripet på grundval av bestämmelser som ska införas i administrativa överenskommelser, t.ex. samförståndsavtal, som föreskriver verkställbara och faktiska rättigheter för de registrerade. Tillstånd från den behöriga tillsynsmyndigheten bör erhållas när skyddsåtgärder föreskrivs i icke rättsligt bindande administrativa arrangemang.
- (109) Personuppgiftsansvarigas eller personuppgiftsbitrådets möjlighet att använda standardiserade dataskyddsbestämmelser som antagits av kommissionen eller av en tillsynsmyndighet bör inte hindra att de infogar

⁽¹⁾ Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

standardiserade dataskyddsbestämmelser i ett vidare avtal, såsom ett avtal mellan personuppgiftsbiträdet och ett annat personuppgiftsbiträde, eller lägger till andra bestämmelser eller ytterligare skyddsåtgärder, under förutsättning att de inte direkt eller indirekt står i strid med standardavtalsklausuler som antagits av kommissionen eller av en tillsynsmyndighet eller påverkar de registrerades grundläggande rättigheter eller friheter. Personuppgiftsansvariga och personuppgiftsbiträden bör uppmuntras att tillhandahålla ytterligare skyddsåtgärder via avtalsmässiga åtaganden som kompletterar de standardiserade skyddsbestämmelserna.

- (110) En koncern eller en grupp av företag som deltar i en gemensam ekonomisk verksamhet bör kunna använda sig av godkända bindande företagsbestämmelser för sina internationella överföringar från unionen till organisationer inom samma koncern eller grupp av företag som deltar i en gemensam ekonomisk verksamhet, under förutsättning att företagsbestämmelserna inbegriper alla nödvändiga principer och bindande rättigheter som säkerställer lämpliga skyddsåtgärder för överföringar eller kategorier av överföringar av personuppgifter.
- (111) Det bör införas bestämmelser som ger möjlighet att under vissa omständigheter göra överföringar, om den registrerade har lämnat sitt uttryckliga samtycke, när överföringen är tillfällig och nödvändig med hänsyn till ett avtal eller ett rättsligt anspråk, oavsett om detta sker inom ett rättsligt förfarande eller i ett administrativt eller utomrättsligt förfarande, inbegripet förfaranden inför tillsynsorgan. Det bör också införas bestämmelser som ger möjlighet till överföringar om viktiga allmänintressen fastställda genom unionsrätten eller medlemsstaternas nationella rätt så kräver eller när överföringen görs från ett register som inrättats genom lag och är avsett att konsulteras av allmänheten eller av personer med ett berättigat intresse. I sistnämnda fall bör en sådan överföring inte omfatta alla personuppgifter eller hela kategorier av uppgifter i registret, och överföringen bör endast göras när registret är avsett att vara tillgängligt för personer med ett berättigat intresse, på begäran av dessa personer eller om de själva är mottagarna, med full hänsyn till de registrerades intressen och grundläggande rättigheter.
- (112) Dessa undantag bör främst vara tillämpliga på uppgiftsöverföringar som krävs och är nödvändiga med hänsyn till viktiga allmänintressen, exempelvis vid internationella utbyten av uppgifter mellan konkurrensmyndigheter, skatte- eller tullmyndigheter, finansstillsynsmyndigheter, socialförsäkringsmyndigheter eller hälsovårdsmyndigheter, till exempel vid kontaktspårning för smittsamma sjukdomar eller för att minska och/eller undanröja dopning inom idrott. En överföring av personuppgifter bör också betraktas som laglig, om den är nödvändig för att skydda ett intresse som är väsentligt för den registrerade eller en annan persons vitala intressen, inklusive dennes fysiska integritet och liv, om den registrerade är oförmögen att ge sitt samtycke. Saknas beslut om adekvat skyddsnivå får unionsrätten eller medlemsstaternas nationella rätt med hänsyn till viktiga allmänintressen uttryckligen fastställa gränser för överföringen av särskilda kategorier av uppgifter till ett tredjeland eller en internationell organisation. Medlemsstaterna bör underrätta kommissionen om sådana bestämmelser. Varje överföring till en internationell humanitär organisation av personuppgifter rörande en registrerad som är fysiskt eller rättsligt förhindrad att ge sitt samtycke, i syfte att utföra en uppgift inom ramen för Genèvekonventionerna eller vara förenlig med internationell humanitär rätt, vilken är tillämplig vid väpnade konflikter, skulle kunna anses vara nödvändig för ett betydande allmänintresse eller för att den är av vitalt intresse för den registrerade.
- (113) Överföringar som kan anses vara icke återkommande och endast gäller ett begränsat antal registrerade kan också vara möjliga när personuppgiftsansvarigas tvingande berättigade intressen motiverar detta, om inte den registrerades intressen eller rättigheter och friheter väger tyngre än dessa intressen, och den personuppgiftsansvarige har bedömt alla omständigheter kring uppgiftsöverföringen. Den personuppgiftsansvarige bör ta särskild hänsyn till personuppgifternas art, den eller de avsedda behandlingarnas ändamål och varaktighet samt situationen i ursprungslandet, tredjelandet och det slutliga bestämmelselandet och bör tillhandahålla lämpliga åtgärder för att skydda fysiska personers grundläggande rättigheter och friheter vid behandlingen av deras personuppgifter. Sådana överföringar bör endast vara möjliga i vissa fall där inget av de andra skälen till överföring är tillämpligt. För vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör hänsyn tas till samhällets legitima förväntningar i fråga om ökad kunskap. Den personuppgiftsansvarige bör informera tillsynsmyndigheten och den registrerade om överföringen.
- (114) Om kommissionen inte har fattat beslut om adekvat dataskyddsnivå i ett tredjeland, bör den personuppgiftsansvarige eller personuppgiftsbiträdet i alla fall använda sig av lösningar som ger de registrerade verkställbara och effektiva rättigheter vad gäller behandlingen av deras personuppgifter inom unionen när dessa uppgifter väl har överförts, så att de fortsatt kan utöva sina grundläggande rättigheter och att skyddsåtgärder fortsatt gäller i förhållande till dem.

- (115) Vissa tredjeländer antar lagar och andra författningar som syftar till att direkt reglera behandling som genomförs av fysiska och juridiska personer under medlemsstaternas jurisdiktion. Detta kan inkludera rättsliga avgöranden eller beslut av administrativa myndigheter i tredjeländer med krav på att personuppgiftsansvariga eller personuppgiftsbiträden överför eller överlämnar personuppgifter, vilka inte grundar sig på något gällande internationellt avtal, såsom ett fördrag om ömsesidig rättshjälp, mellan det begärande tredjelandet och unionen eller en medlemsstat. Extraterritoriell tillämpning av dessa lagar och andra författningar kan strida mot internationell rätt och inverka menligt på det skydd av fysiska personer som säkerställs inom unionen genom denna förordning. Överföringar bör endast tillåtas om villkoren i denna förordning för en överföring till tredjeländer är uppfyllda. Detta kan vara fallet bl.a. när utlämnande är nödvändigt på grund av ett viktigt allmänintresse som erkänns i unionsrätten eller i medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av.
- (116) När personuppgifter förs över gränser utanför unionen kan detta öka risken för att fysiska personer inte kan utöva sina dataskyddsrättigheter, i synnerhet för att skydda sig från otillåten användning eller otillåtet utlämnande av denna information. Samtidigt kan tillsynsmyndigheter finna att de inte är i stånd att handlägga klagomål eller göra utredningar som gäller verksamheter utanför gränserna för deras land. Deras strävan att arbeta tillsammans över gränserna kan också hindras av otillräckliga preventiva eller korrigerande befogenheter, oenhetliga rättsliga regelverk och praktiska hinder, som exempelvis bristande resurser. Närmare samarbete mellan dataskyddstillsynsmyndigheter bör därför främjas för att hjälpa dem att utbyta information och utföra utredningar med sina internationella motparter. I syfte att bygga upp internationella samarbetsmekanismer för att underlätta och tillhandahålla ömsesidig internationell hjälp med att kontrollera efterlevnaden av lagstiftningen till skydd för personuppgifter, bör kommissionen och tillsynsmyndigheterna utbyta information och samarbeta, inom verksamhet som rör utövandet av deras befogenheter, med behöriga myndigheter i tredjeländer, på grundval av ömsesidighet och i överensstämmelse med denna förordning.
- (117) Ett väsentligt inslag i skyddet av fysiska personer vid behandlingen av personuppgifter är att medlemsstaterna inrättar tillsynsmyndigheter med behörighet att utföra sina uppgifter och utöva sina befogenheter under fullständigt oberoende. Medlemsstaterna bör kunna inrätta fler än en tillsynsmyndighet om det behövs för att ta hänsyn till den egna konstitutionella, organisatoriska och administrativa strukturen.
- (118) Tillsynsmyndigheternas oberoende bör dock inte innebära att deras utgifter inte kan underkastas kontroll- eller övervakningsmekanismer eller bli föremål för domstolsprövning.
- (119) Om en medlemsstat inrättar flera tillsynsmyndigheter, bör den genom lagstiftning säkerställa att dessa tillsynsmyndigheter effektivt deltar i mekanismen för enhetlighet. Medlemsstaten bör i synnerhet utnämna en tillsynsmyndighet som fungerar som samlande kontaktpunkt för dessa myndigheters effektiva deltagande i mekanismen för att säkra ett snabbt och smidigt samarbete med övriga tillsynsmyndigheter, styrelsen och kommissionen.
- (120) Varje tillsynsmyndighet bör tilldelas de ekonomiska och personella resurser och lokalutrymmen samt den infrastruktur som är nödvändig för att den effektivt ska kunna utföra sina uppgifter, däribland de uppgifter som är knutna till ömsesidigt bistånd och samarbete med övriga tillsynsmyndigheter i hela unionen. Varje tillsynsmyndighet bör ha en separat offentlig årlig budget, som kan ingå i den övergripande statsbudgeten eller nationella budgeten.
- (121) De allmänna villkoren för tillsynsmyndighetens ledamot eller ledamöter bör fastställas genom varje medlemsstats lagstiftning och där bör i synnerhet föreskrivas att ledamöterna ska utnämnas genom ett öppet förfarande antingen av medlemsstatens parlament, regering eller statschef, på grundval av ett förslag från regeringen, en ledamot av regeringen, parlamentet eller en av parlamentets kammare eller av ett oberoende organ som enligt medlemsstaternas nationella rätt har anförtratts utnämningen. I syfte att säkerställa tillsynsmyndighetens oberoende bör ledamoten eller ledamöterna handla med integritet, avstå från alla handlingar som står i strid med deras tjänsteutövning och under sin mandattid avstå från all annan avlönad eller oavlönad yrkesverksamhet som står i strid med deras uppdrag. Tillsynsmyndigheten bör ha egen personal, som valts ut av tillsynsmyndigheten eller ett oberoende organ som fastställs i medlemsstaternas nationella rätt, vilken uteslutande bör vara underställd tillsynsmyndighetens ledamot eller ledamöter.
- (122) Varje tillsynsmyndighet bör ha behörighet att inom sin medlemsstats territorium utöva de befogenheter och utföra de uppgifter som den tilldelats i enlighet med denna förordning. Detta bör framför allt omfatta behandling

inom ramen för verksamhet vid den personuppgiftsansvariges eller personuppgiftsbitrådets verksamhetsställen inom den egna medlemsstatens territorium, behandling av personuppgifter som utförs av myndigheter eller privata organ som agerar i ett allmänt intresse, behandling som påverkar registrerade på dess territorium eller behandling som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad i unionen när den rör registrerade som är bosatta på dess territorium. Detta bör inbegripa att hantera klagomål som lämnas in av en registrerad, genomföra undersökningar om tillämpningen av denna förordning samt främja allmänhetens medvetenhet om risker, bestämmelser, skyddsåtgärder och rättigheter när det gäller behandlingen av personuppgifter.

- (123) Tillsynsmyndigheterna bör övervaka tillämpningen av bestämmelserna i denna förordning och bidra till att tillämpningen blir enhetlig över hela unionen, för att skydda fysiska personer vid behandling av deras personuppgifter och för att underlätta det fria flödet av personuppgifter inom den inre marknaden. För detta ändamål bör tillsynsmyndigheterna samarbeta såväl sinsemellan som med kommissionen, utan att det behövs något avtal mellan medlemsstaterna om tillhandahållande av ömsesidigt bistånd eller om sådant samarbete.
- (124) Om behandlingen av personuppgifter sker inom ramen för verksamhet vid en personuppgiftsansvarigs eller ett personuppgiftsbitrådes verksamhetsställe i unionen och den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad i mer än en medlemsstat, eller om behandling som sker inom ramen för verksamhet vid ett enda verksamhetsställe tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen i väsentlig grad påverkar eller sannolikt i väsentlig grad kommer att påverka registrerade i mer än en medlemsstat, bör tillsynsmyndigheten för den personuppgiftsansvariges eller personuppgiftsbitrådets huvudsakliga verksamhetsställe eller för detta enda verksamhetsställe tillhörande den personuppgiftsansvarige eller personuppgiftsbiträdet agera som ansvarig myndighet. Denna bör samarbeta med de övriga myndigheter som berörs, eftersom den personuppgiftsansvarige eller personuppgiftsbiträdet har ett verksamhetsställe inom deras medlemsstats territorium, eftersom registrerade som är bosatta på deras territorium i väsentlig grad påverkas eller eftersom ett klagomål har lämnats in till dem. Även när en registrerad som inte är bosatt i medlemsstaten har lämnat in ett klagomål, bör den tillsynsmyndighet som klagomålet har lämnats in till också vara en berörd tillsynsmyndighet. Styrelsen bör inom ramen för sina uppgifter kunna utfärda riktlinjer för alla frågor som rör tillämpningen av denna förordning, framför allt för vilka kriterier som ska beaktas för att konstatera om behandlingen i fråga i väsentlig grad påverkar registrerade i mer än en medlemsstat och för vad som utgör en relevant och motiverad invändning.
- (125) Den ansvariga myndigheten bör ha behörighet att anta bindande beslut om åtgärder inom ramen för de befogenheter som den tilldelats i enlighet med denna förordning. I egenskap av ansvarig myndighet bör tillsynsmyndigheten nära involvera och samordna de berörda tillsynsmyndigheterna i beslutsfattandet. Om man beslutar att helt eller delvis avslå den registrerades klagomål, bör detta beslut antas av den tillsynsmyndighet som klagomålet har lämnats in till.
- (126) Den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna bör gemensamt enas om beslutet, som bör rikta sig till den personuppgiftsansvariges eller personuppgiftsbitrådets huvudsakliga eller enda verksamhetsställe och vara bindande för den personuppgiftsansvarige och personuppgiftsbiträdet. Den personuppgiftsansvarige eller personuppgiftsbiträdet bör vidta de åtgärder som krävs för att säkerställa efterlevnad av denna förordning och genomförande av det beslut som den ansvariga tillsynsmyndigheten har anmält till den personuppgiftsansvariges eller personuppgiftsbitrådets huvudsakliga verksamhetsställe vad gäller behandling i unionen.
- (127) Varje tillsynsmyndighet som inte agerar som ansvarig tillsynsmyndighet bör vara behörig att behandla lokala fall, om den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad i mer än en medlemsstat men ärendet för den specifika behandlingen endast avser behandling som utförs i en enda medlemsstat och endast omfattar registrerade i denna enda medlemsstat, till exempel om ärendet avser behandling av anställdas personuppgifter inom ramen för en medlemsstats specifika anställningsförhållanden. I sådana fall bör tillsynsmyndigheten utan dröjsmål underrätta den ansvariga tillsynsmyndigheten om detta ärende. Efter att ha underrättats bör den ansvariga tillsynsmyndigheten besluta huruvida den kommer att hantera ärendet i enlighet med bestämmelsen om samarbete mellan den ansvariga tillsynsmyndigheten och andra berörda tillsynsmyndigheter (nedan kallad *mekanismen för en enda kontaktpunkt*), eller om den tillsynsmyndighet som underrättade den bör behandla ärendet på lokal nivå. När den ansvariga tillsynsmyndigheten beslutar huruvida den kommer att behandla ärendet, bör den ta hänsyn till om den personuppgiftsansvarige eller personuppgiftsbiträdet har ett verksamhetsställe i den medlemsstat där den tillsynsmyndighet som underrättade den ansvariga myndigheten är belägen för att säkerställa ett effektivt genomförande av ett beslut gentemot den personuppgiftsansvarige eller personuppgiftsbiträdet. När den ansvariga tillsynsmyndigheten beslutar att behandla ärendet, bör den tillsynsmyndighet som underrättade den

ha möjlighet att lämna in ett förslag till beslut, som den ansvariga tillsynsmyndigheten bör ta största möjliga hänsyn till när den utarbetar utkastet till beslut inom ramen för mekanismen för en enda kontaktpunkt.

- (128) Bestämmelserna om den ansvariga tillsynsmyndigheten och mekanismen för en enda kontaktpunkt bör inte tillämpas om behandlingen utförs av myndigheter eller privata organ i ett allmänt intresse. I sådana fall bör den enda tillsynsmyndighet som är behörig att utöva de befogenheter som den tilldelas i enlighet med denna förordning vara tillsynsmyndigheten i den medlemsstat där myndigheten eller det privata organet är etablerat.
- (129) För att denna förordning ska övervakas och verkställas på ett enhetligt sätt i hela unionen bör tillsynsmyndigheterna i alla medlemsstater ha samma uppgifter och effektiva befogenheter, bl.a. undersökningsbefogenheter, korrigerande befogenheter och befogenheter att ålägga sanktioner samt befogenheter att utfärda tillstånd och ge råd, särskilt vid klagomål från fysiska personer och, utan att det påverkar åklagarmyndigheternas befogenheter enligt medlemsstaternas nationella rätt, att upplysa de rättsliga myndigheterna om överträdelser av denna förordning och delta i rättsliga förfaranden. Dessa befogenheter bör även omfatta en befogenhet att införa en tillfällig eller definitiv begränsning av, inklusive förbud mot, behandling. Medlemsstaterna får fastställa andra uppgifter med anknytning till skyddet av personuppgifter enligt denna förordning. Tillsynsmyndigheternas befogenheter bör utövas opartiskt, rättvist och inom rimlig tid i överensstämmelse med lämpliga rättssäkerhetsgarantier i unionsrätten och i medlemsstaternas nationella rätt. Framför allt bör varje åtgärd vara lämplig, nödvändig och proportionell för att säkerställa efterlevnad av denna förordning, med beaktande av omständigheterna i varje enskilt fall, samt respektera varje persons rätt att bli hörd innan några enskilda åtgärder som påverkar honom eller henne negativt vidtas och vara utformad så att onödiga kostnader och alltför stora olägenheter för de berörda personerna undviks. Undersökningsbefogenheten när det gäller tillträde till lokaler bör utövas i enlighet med särskilda krav i medlemsstaternas nationella processrätt, såsom kravet på att inhämta förhandstillstånd från rättsliga myndigheter. Varje rättsligt bindande åtgärd som vidtas av tillsynsmyndigheten bör vara skriftlig, klar och entydig, innehålla information om vilken tillsynsmyndighet som har utfärdat åtgärden och datum för utfärdandet, vara undertecknad av tillsynsmyndighetens chef eller en av dess ledamöter efter dennes bemyndigande samt innehålla en motivering till åtgärden och en hänvisning till rätten till ett effektivt rättsmedel. Detta bör inte utesluta ytterligare krav enligt medlemsstaternas nationella processrätt. Antagande av ett rättsligt bindande beslut innebär att det kan bli föremål för domstolsprövning i den medlemsstat till vilken den tillsynsmyndighet som antog beslutet hör.
- (130) Om den tillsynsmyndighet till vilken klagomålet har ingetts inte är den ansvariga tillsynsmyndigheten, bör den ansvariga tillsynsmyndigheten nära samarbeta med den tillsynsmyndighet till vilken klagomålet har ingetts i enlighet med de bestämmelser om samarbete och enhetlighet som fastställs i denna förordning. I sådana fall bör den ansvariga tillsynsmyndigheten när den vidtar åtgärder avsedda att ha rättsverkan, inbegripet utdömandet av administrativa sanktionsavgifter, ta största hänsyn till synpunkter från den tillsynsmyndighet till vilken klagomålet har ingetts, vilken bör kvarstå som behörig för genomförande av utredningar på den egna medlemsstatens territorium i samverkan med den behöriga tillsynsmyndigheten.
- (131) Om en annan tillsynsmyndighet bör agera som ansvarig tillsynsmyndighet för den personuppgiftsansvariges eller personuppgiftsbitrådets behandling men den sakfråga som klagomålet gäller eller den möjliga överträdelsen endast rör den personuppgiftsansvariges eller personuppgiftsbitrådets behandling i den medlemsstat där klagomålet har ingetts eller den eventuella överträdelsen har upptäckts, och frågan inte i väsentlig grad påverkar eller inte sannolikt i väsentlig grad kommer att påverka registrerade i andra medlemsstater, bör den tillsynsmyndighet som mottar ett klagomål eller upptäcker eller på annat sätt informeras om situationer som innebär eventuella överträdelser av denna förordning försöka få till stånd en uppgörelse i godo med den personuppgiftsansvarige och, om detta inte lyckas, utöva sina befogenheter fullt ut. Detta bör omfatta särskild behandling som utförs inom tillsynsmyndighetens medlemsstats territorium eller med avseende på registrerade inom denna medlemsstats territorium, behandling som utförs inom ramen för ett erbjudande om varor eller tjänster som särskilt riktar sig till registrerade inom tillsynsmyndighetens medlemsstats territorium eller behandling som måste bedömas med beaktande av relevanta rättsliga skyldigheter enligt medlemsstaternas nationella rätt.
- (132) Medvetandehöjande kampanjer från tillsynsmyndigheters sida riktade till allmänheten bör innefatta särskilda åtgärder riktade dels till personuppgiftsansvariga och personuppgiftsbitråden, inbegripet mikroföretag samt små och medelstora företag, dels till fysiska personer, särskilt i utbildningssammanhang.

- (133) Tillsynsmyndigheterna bör hjälpa varandra att utföra sina uppgifter och ge ömsesidigt bistånd så att denna förordning tillämpas och verkställs enhetligt på den inre marknaden. En tillsynsmyndighet som begärt ömsesidigt bistånd får anta en provisorisk åtgärd, om den inte har fått något svar på en begäran om ömsesidigt bistånd inom en månad från det att begäran mottogs av den andra tillsynsmyndigheten.
- (134) Alla tillsynsmyndigheter bör om lämpligt delta i gemensamma insatser med andra tillsynsmyndigheter. Den anmodade tillsynsmyndigheten bör vara skyldig att besvara en begäran inom en fastställd tidsperiod.
- (135) För att denna förordning ska tillämpas enhetligt i hela unionen bör en mekanism för enhetlighet när det gäller samarbete mellan tillsynsmyndigheterna skapas. Denna mekanism bör främst tillämpas när en tillsynsmyndighet avser att anta en åtgärd som är avsedd att ha rättsverkan gällande behandlingar som i väsentlig grad påverkar ett betydande antal registrerade i flera medlemsstater. Den bör också tillämpas när en berörd tillsynsmyndighet eller kommissionen begär att ett sådant ärende ska hanteras inom ramen för mekanismen för enhetlighet. Mekanismen bör inte påverka åtgärder som kommissionen kan komma att vidta när den utövar sina befogenheter enligt fördragen.
- (136) Vid tillämpningen av mekanismen för enhetlighet bör styrelsen inom en fastställd tidsperiod avge ett yttrande, om en majoritet av dess ledamöter så beslutar eller om någon berörd tillsynsmyndighet eller kommissionen begär detta. Styrelsen bör också ges befogenhet att anta rättsligt bindande beslut vid tvister mellan tillsynsmyndigheter. För detta ändamål bör den, normalt med två tredjedelars majoritet av sina ledamöter, utfärda rättsligt bindande beslut i tydligt fastställda fall då tillsynsmyndigheter har olika uppfattningar, framför allt när det gäller mekanismen för samarbete mellan den ansvariga tillsynsmyndigheten och berörda tillsynsmyndigheter om sakförhållandena, i synnerhet om huruvida denna förordning har överträtts.
- (137) Det kan uppstå brådskande behov att agera för att skydda registrerades rättigheter och friheter, särskilt när fara föreligger att säkerställandet av en registrerad persons rättighet kan komma att försvåras avsevärt. En tillsynsmyndighet bör därför kunna vidta vederbörligen motiverade provisoriska åtgärder inom sitt territorium med en viss giltighetsperiod, som inte bör överskrida tre månader.
- (138) Tillämpningen av en sådan mekanism bör vara ett villkor för lagligheten av en åtgärd som är avsedd att ha rättsverkan och som vidtas av tillsynsmyndigheten i de fall där denna tillämpning är obligatorisk. I andra ärenden som inbegriper flera länder bör samarbetsmekanismen mellan den ansvariga tillsynsmyndigheten och berörda tillsynsmyndigheter tillämpas, och ömsesidigt bistånd och gemensamma insatser kan utföras mellan de berörda tillsynsmyndigheterna på bilateral eller multilateral basis utan att mekanismen för enhetlighet utlöses.
- (139) I syfte att främja en enhetlig tillämpning av denna förordning bör styrelsen inrättas som ett oberoende unionsorgan. För att styrelsen ska kunna uppfylla sina mål bör den vara en juridisk person. Styrelsen bör företrädas av sin ordförande. Den bör ersätta arbetsgruppen för skydd av fysiska personer med avseende på behandlingen av personuppgifter, som inrättades genom direktiv 95/46/EG. Den bör bestå av chefen för en tillsynsmyndighet i varje medlemsstat och Europeiska datatillsynsmannen eller deras respektive företrädare. Kommissionen bör delta i styrelsens verksamhet utan att ha rösträtt, och Europeiska datatillsynsmannen bör ha specifik rösträtt. Styrelsen bör bidra till denna förordnings enhetliga tillämpning i hela unionen, bl.a. genom att lämna råd till kommissionen, särskilt vad gäller skyddsnivån i tredjeländer eller internationella organisationer, och främja samarbetet mellan tillsynsmyndigheterna i hela unionen. Styrelsen bör agera oberoende när den utför sina uppgifter.
- (140) Styrelsen bör biträdas av ett sekretariat som tillhandahålls av Europeiska datatillsynsmannen. Den personal vid Europeiska datatillsynsmannen som medverkar i utförandet av de uppgifter som enligt denna förordning anförtros styrelsen bör för sina uppgifter uteslutande ta emot instruktioner från styrelsens ordförande och rapportera till denne.
- (141) Alla registrerade bör ha rätt att lämna in ett klagomål till en enda tillsynsmyndighet, särskilt i den medlemsstat där den registrerade har sin hemvist, och ha rätt till ett effektivt rättsmedel i enlighet med artikel 47 i stadgan,

om den registrerade anser att hans eller hennes rättigheter enligt denna förordning har kränkts eller om tillsynsmyndigheten inte reagerar på ett klagomål, helt eller delvis avslår eller avvisar ett klagomål eller inte agerar när så är nödvändigt för att skydda den registrerades rättigheter. Utredningen av ett klagomål bör, med förbehåll för eventuell domstolsprövning, ske i den utsträckning som är lämplig i det enskilda fallet. Tillsynsmyndigheten bör inom rimlig tid informera den registrerade om hur arbetet med klagomålet fortskrider och vad resultatet blir. Om ärendet fordrar ytterligare utredning eller samordning med en annan tillsynsmyndighet, bör den registrerade underrättas även om detta. För att förenkla inlämningen av klagomål bör varje tillsynsmyndighet vidta åtgärder, såsom att tillhandahålla ett formulär för inlämnande av klagomål som även kan fyllas i elektroniskt, utan att andra kommunikationsformer utesluts.

- (142) Om en registrerad anser att hans eller hennes rättigheter enligt denna förordning har kränkts, bör han eller hon ha rätt att ge mandat till ett organ, en organisation eller en sammanslutning som drivs utan vinstsyfte och som har inrättats i enlighet med en medlemsstats nationella rätt, som har stadgeenliga mål av allmänt intresse och bedriver verksamhet på området skydd av personuppgifter, att på hans eller hennes vägnar lämna in ett klagomål till en tillsynsmyndighet, om detta föreskrivs i medlemsstatens nationella rätt, att på den registrerades vägnar utöva rätten till domstolsprövning eller att på den registrerades vägnar utöva rätten att ta emot ersättning. En medlemsstat får föreskriva att ett sådant organ, en sådan organisation eller en sådan sammanslutning ska ha rätt att lämna in ett klagomål i den medlemsstaten, oberoende av en registrerad persons mandat, och ha rätt till ett effektivt rättsmedel, om det eller den har skäl att anse att en registrerad persons rättigheter har kränkts till följd av behandling av personuppgifter som strider mot denna förordning. Detta organ, denna organisation eller denna sammanslutning får inte ges rätt att kräva ersättning på en registrerad persons vägnar oberoende av den registrerades mandat.
- (143) Varje fysisk eller juridisk person har rätt att väcka ogiltighetstalan mot styrelsens beslut vid domstolen enligt de villkor som föreskrivs i artikel 263 i EUF-fördraget. I sin egenskap av adressater för sådana beslut måste, i enlighet med artikel 263 i EUF-fördraget, de berörda tillsynsmyndigheter som önskar överklaga dessa väcka talan inom två månader efter det att beslutet meddelats dem. Om styrelsens beslut direkt och personligen berör en personuppgiftsansvarig, ett personuppgiftsbiträde eller en enskild, kan den enskilde väcka ogiltighetstalan mot beslutet inom två månader efter det att de har offentliggjorts på styrelsens webbplats, i enlighet med artikel 263 i EUF-fördraget. Utan att det påverkar denna rätt inom ramen för artikel 263 i EUF-fördraget bör varje fysisk eller juridisk person ha rätt till ett effektivt rättsmedel vid den behöriga nationella domstolen mot ett beslut av en tillsynsmyndighet som har rättsliga följder för denna person. Sådana beslut avser särskilt tillsynsmyndighetens utövande av utrednings-, korrigerings- och godkännandebefogenheter eller avvisande av eller avslag på klagomål. Rätten till ett effektivt rättsmedel inbegriper dock inte åtgärder som vidtagits av tillsynsmyndigheter när dessa inte är rättsligt bindande, såsom yttranden som avgivits eller rådgivning som tillhandahållits av tillsynsmyndigheten. Talan mot beslut som har fattats av en tillsynsmyndighet bör väckas vid domstolarna i den medlemsstat där tillsynsmyndigheten har sitt säte och bör genomföras i enlighet med den medlemsstatens nationella processrätt. Dessa domstolar bör ha fullständig behörighet, vilket bör omfatta behörighet att pröva alla fakta och rättsliga frågor som rör den tvist som anhängiggjorts vid dem.

Om talan avslås eller avvisas av en tillsynsmyndighet, kan den enskilde väcka talan vid domstolarna i samma medlemsstat. I samband med rättsmedel som avser tillämpningen av denna förordning kan eller, i det fall som anges i artikel 267 i EUF-fördraget, måste nationella domstolar som anser att ett beslut om ett förhandsavgörande är nödvändigt för att de ska kunna döma begära att domstolen meddelar ett förhandsavgörande om tolkningen av unionsrätten, inbegripet denna förordning. Om dessutom ett beslut av en tillsynsmyndighet om genomförande av ett beslut av styrelsen överklagas till en nationell domstol och giltigheten av styrelsens beslut ifrågasätts, har inte den nationella domstolen befogenhet att förklara styrelsens beslut ogiltigt utan måste hänskjuta frågan om giltighet till domstolen i enlighet med artikel 267 i EUF-fördraget såsom den tolkats av domstolen, närhelst den anser att beslutet är ogiltigt. En nationell domstol får dock inte hänskjuta en fråga om giltigheten av styrelsens beslut på begäran av en fysisk eller juridisk person som haft tillfälle att väcka ogiltighetstalan mot beslutet, i synnerhet inte om denna person direkt och personligen berördes av beslutet men inte gjorde detta inom den frist som anges i artikel 263 i EUF-fördraget.

- (144) Om en domstol där ett förfarande inletts mot beslut som har fattats av en tillsynsmyndighet har skäl att tro att ett förfarande rörande samma behandling, såsom samma sakfråga vad gäller behandling av samma personuppgiftsansvarige eller samma personuppgiftsbiträde, eller samma händelseförlopp, har inletts vid en annan behörig domstol i en annan medlemsstat, bör den kontakta denna domstol i syfte att bekräfta förekomsten av sådana relaterade förfaranden. Om relaterade förfaranden pågår vid en domstol i en annan medlemsstat får alla andra

domstolar än den domstol där förfarandet först inleddes låta förfarandena vila eller på en av parternas begäran förklara sig obehöriga till förmån för den domstol där förfarandet först inleddes, om den domstolen har behörighet i förfarandet i fråga och dess lagstiftning tillåter förening av sådana relaterade förfaranden. Förfarandena anses vara relaterade, om de är så nära förenade att en gemensam handläggning och dom är påkallad för att undvika att oförenliga domar meddelas som en följd av att förfarandena prövas i olika rättegångar.

- (145) När det gäller ett rättsligt förfarande mot en personuppgiftsansvarig eller ett personuppgiftsbiträde bör käranden kunna välja att väcka talan antingen vid domstolarna i de medlemsstater där den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad eller där den registrerade är bosatt, såvida inte den personuppgiftsansvarige är en myndighet i en medlemsstat som agerar inom ramen för sin myndighetsutövning.
- (146) Den personuppgiftsansvarige eller personuppgiftsbiträdet bör ersätta all skada som en person kan komma att lida till följd av behandling som strider mot denna förordning. Den personuppgiftsansvarige eller personuppgiftsbiträdet bör dock befrias från skadeståndsskyldighet om den kan visa att den inte på något sätt är ansvarig för skadan. Begreppet skada bör tolkas brett mot bakgrund av domstolens rättspraxis på ett sätt som fullt ut återspeglar denna förordnings mål. Detta påverkar inte skadeståndsanspråk till följd av överträdelser av andra bestämmelser i unionsrätten eller i medlemsstaternas nationella rätt. Behandling som strider mot denna förordning omfattar även behandling som strider mot delegerade akter och genomförandekter som antagits i enlighet med denna förordning och medlemsstaternas nationella rätt med närmare specifikation av denna förordnings bestämmelser. Registrerade bör få full och effektiv ersättning för den skada de lidit. Om personuppgiftsansvariga eller personuppgiftsbiträden medverkat vid samma behandling, bör varje personuppgiftsansvarig eller personuppgiftsbiträde hållas ansvarig för hela skadan. Om de är förenade i samma rättsliga förfarande i enlighet med medlemsstaternas nationella rätt, kan ersättningen dock fördelas i enlighet med varje personuppgiftsansvarigs eller personuppgiftsbiträdes ansvar för den genom behandlingen uppkomna skadan, förutsatt att den registrerade som lidit skada tillförsäkras full och effektiv ersättning. Varje personuppgiftsansvarig eller personuppgiftsbiträde som har betalat full ersättning får därefter inleda förfaranden för återkrav mot andra personuppgiftsansvariga eller personuppgiftsbiträden som medverkat vid samma behandling.
- (147) Om särskilda bestämmelser om behörighet fastställs i denna förordning, framför allt vad gäller förfaranden för att begära rättslig prövning som inbegriper ersättning mot en personuppgiftsansvarig eller ett personuppgiftsbiträde, bör inte allmänna bestämmelser om behörighet, såsom bestämmelserna i Europaparlamentets och rådets förordning (EU) nr 1215/2012⁽¹⁾, påverka tillämpningen av sådana särskilda bestämmelser.
- (148) För att stärka verkställigheten av denna förordning bör det utdömas sanktioner, inbegripet administrativa sanktionsavgifter, för överträdelser av denna förordning utöver eller i stället för de lämpliga åtgärder som tillsynsmyndigheten vidtar i enlighet med denna förordning. Vid en mindre överträdelse eller om den sanktionsavgift som sannolikt skulle utdömas skulle innebära en oproportionell börda för en fysisk person får en reprimand utfärdas i stället för sanktionsavgifter. Vederbörlig hänsyn bör dock tas till överträdelsens karaktär, svårighetsgrad och varaktighet och huruvida den har skett uppsåtligen, vilka åtgärder som vidtagits för att lindra skadan, graden av ansvar eller eventuella tidigare överträdelser av relevans, det sätt på vilket överträdelsen kom till tillsynsmyndighetens kännedom, efterlevnad av åtgärder som förordnats mot den personuppgiftsansvarige eller personuppgiftsbiträdet, tillämpning av en uppförandekod och eventuella andra försvärande eller förmildrande faktorer. Utdömandet av sanktioner, inbegripet administrativa sanktionsavgifter, bör underkastas adekvata rättssäkerhetsgarantier i överensstämmelse med allmänna principer inom unionsrätten och stadgan, vilket inbegriper ett effektivt rättsligt skydd och korrekt rättsligt förfarande.
- (149) Medlemsstaterna bör kunna fastställa bestämmelser om straffrättsliga påföljder för överträdelser av denna förordning, inbegripet för överträdelser av nationella bestämmelser som antagits i enlighet med och inom ramen för denna förordning. Dessa straffrättsliga påföljder kan även inbegripa en möjlighet att förverka den vinning som gjorts genom överträdelser av denna förordning. Utdömandet av straffrättsliga påföljder för överträdelser av sådana nationella bestämmelser och administrativa sanktioner bör dock inte medföra ett åsidosättande av principen *ne bis in idem* enligt domstolens tolkning.
- (150) För att förstärka och harmonisera de administrativa sanktionerna för överträdelser av denna förordning bör samtliga tillsynsmyndigheter ha befogenhet att utfärda administrativa sanktionsavgifter. Det bör i denna

⁽¹⁾ Europaparlamentets och rådets förordning (EU) nr 1215/2012 av den 12 december 2012 om domstols behörighet och om erkännande och verkställighet av domar på privaträttens område (EUTL 351, 20.12.2012, s. 1).

förordning anges vilka överträdelserna är, den övre gränsen för och kriterierna för fastställande av de administrativa sanktionsavgifterna, som i varje enskilt fall bör bestämmas av den behöriga tillsynsmyndigheten med beaktande av alla relevanta omständigheter i det särskilda fallet, med vederbörlig hänsyn bl.a. till överträdelsens karaktär, svårighetsgrad och varaktighet samt till dess följder och till de åtgärder som vidtas för att sörja för fullgörandet av skyldigheterna enligt denna förordning och för att förebygga eller lindra konsekvenserna av överträdelsen. Om de administrativa sanktionsavgifterna åläggs ett företag, bör ett företag i detta syfte anses vara ett företag i den mening som avses i artiklarna 101 och 102 i EUF-fördraget. Om de administrativa sanktionsavgifterna åläggs personer som inte är ett företag, bör tillsynsmyndigheten ta hänsyn till den allmänna inkomstnivån i medlemsstaten och personens ekonomiska situation, när den överväger lämplig sanktionsavgift. Mekanismen för enhetlighet kan också tillämpas för att främja en enhetlig tillämpning av administrativa sanktionsavgifter. Medlemsstaterna bör fastställa om och i vilken utsträckning myndigheter ska omfattas av administrativa sanktionsavgifter. Utfärdande av administrativa sanktionsavgifter eller utdelning av en varning påverkar inte tillämpningen av tillsynsmyndigheternas övriga befogenheter eller av andra sanktioner enligt denna förordning.

- (151) Danmarks och Estlands rättssystem tillåter inte administrativa sanktionsavgifter i enlighet med denna förordning. Bestämmelserna om administrativa sanktionsavgifter kan tillämpas så att sanktionsavgiften i Danmark utdöms som en straffrättslig påföljd av en behörig nationell domstol och att den i Estland utdöms av tillsynsmyndigheten inom ramen för ett förseelseförfarande, under förutsättning att en sådan tillämpning av bestämmelserna i dessa medlemsstater har en effekt som är likvärdig med administrativa sanktionsavgifter som utdöms av tillsynsmyndigheter. De behöriga nationella domstolarna bör därför beakta rekommendationen från den tillsynsmyndighet som initierar sanktionsavgiften. De sanktionsavgifter som utdöms bör i alla händelser vara effektiva, proportionella och avskräckande.
- (152) Om denna förordning inte harmoniserar administrativa sanktioner eller om nödvändigt i andra fall, till exempel vid fall av allvarliga överträdelser av denna förordning, bör medlemsstaterna genomföra ett system med effektiva, proportionella och avskräckande sanktioner. Dessa sanktioners art, straffrättsliga eller administrativa, bör fastställas i medlemsstaternas nationella rätt.
- (153) Medlemsstaterna bör i sin lagstiftning sammanjämka bestämmelserna om yttrandefrihet och informationsfrihet, vilket inbegriper journalistiska, akademiska, konstnärliga och/eller litterära uttrycksformer, med rätten till skydd av personuppgifter i enlighet med denna förordning. Behandling av personuppgifter enbart för journalistiska, akademiska, konstnärliga eller litterära ändamål bör undantas från vissa av kraven i denna förordning, så att rätten till skydd av personuppgifter vid behov kan förenas med rätten till yttrandefrihet och informationsfrihet, som följer av artikel 11 i stadgan. Detta bör särskilt gälla vid behandling av personuppgifter inom det audiovisuella området och i nyhetsarkiv och pressbibliotek. Medlemsstaterna bör därför anta lagstiftningsåtgärder som fastställer de olika undantag som behövs för att skapa en balans mellan dessa grundläggande rättigheter. Medlemsstaterna bör fastställa sådana undantag med avseende på allmänna principer, de registrerades rättigheter, personuppgiftsansvariga och personuppgiftsbiträden, överföring av uppgifter till tredjeländer eller internationella organisationer, de oberoende tillsynsmyndigheterna, samarbete och enhetlighet samt specifika situationer där personuppgifter behandlas. Om sådana undantag varierar från en medlemsstat till en annan, ska den nationella rätten i den medlemsstat vars lag den personuppgiftsansvarige omfattas av tillämpas. För att beakta vikten av rätten till yttrandefrihet i varje demokratiskt samhälle måste det göras en bred tolkning av vad som innefattas i denna frihet, som till exempel journalistik.
- (154) Denna förordning gör det möjligt att vid tillämpningen av den ta hänsyn till principen om allmänhetens rätt att få tillgång till allmänna handlingar. Allmänhetens rätt att få tillgång till allmänna handlingar kan betraktas som ett allmänt intresse. Personuppgifter i handlingar som innehas av en myndighet eller ett offentligt organ bör kunna lämnas ut offentligt av denna myndighet eller detta organ, om utlämning stadgas i unionsrätten eller i medlemsstatens nationella rätt som är tillämplig på myndigheten eller det offentliga organet. Denna rätt bör sammanjämka allmänhetens rätt att få tillgång till allmänna handlingar och vidareutnyttjande av information från den offentliga sektorn med rätten till skydd av personuppgifter och får därför innehålla föreskrifter om den nödvändiga sammanjämkningen med rätten till skydd av personuppgifter enligt denna förordning. Hänvisningen till offentliga myndigheter och organ bör i detta sammanhang omfatta samtliga myndigheter eller andra organ som omfattas av medlemsstaternas nationella rätt om allmänhetens tillgång till handlingar. Europaparlamentets och rådets direktiv 2003/98/EG ⁽¹⁾ ska inte på något sätt påverka skyddsnivån för fysiska personer med avseende

⁽¹⁾ Europaparlamentets och rådets direktiv 2003/98/EG av den 17 november 2003 om vidareutnyttjande av information från den offentliga sektorn (EUT L 345, 31.12.2003, s. 90).

på behandling av personuppgifter enligt bestämmelserna i unionsrätten och i medlemsstaternas nationella rätt och i synnerhet ändras inte de skyldigheter och rättigheter som anges i denna förordning genom det direktivet. I synnerhet ska direktivet inte vara tillämpligt på handlingar till vilka, med hänsyn till skyddet av personuppgifter, tillgång enligt tillgångsbestämmelserna är utesluten eller begränsad eller på delar av handlingar som är tillgängliga enligt dessa bestämmelser men som innehåller personuppgifter vilkas vidareutnyttjande i lag har fastställts som oförenligt med lagstiftningen om skydd för fysiska personer vid behandling av personuppgifter.

- (155) En medlemsstatsnationella rätt eller kollektivavtal, inbegripet "verksamhetsöverenskommelser", får föreskriva särskilda bestämmelser om behandling av anställdas personuppgifter i anställningsförhållanden, särskilt när det gäller villkoren för hur personuppgifter i anställningsförhållanden får behandlas på grundval av samtycke från den anställde, rekrytering, genomförande av anställningsavtalet, inklusive befrielse från i lag eller kollektivavtal stadgade skyldigheter, ledning, planering och organisering av arbetet samt hälsa och säkerhet på arbetsplatsen, men också när det gäller att såväl kollektivt som individuellt utöva och komma i åtnjutande av rättigheter och förmåner som är knutna till anställningen samt att avsluta anställningsförhållandet.
- (156) Behandlingen av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör omfattas av lämpliga skyddsåtgärder för de registrerades rättigheter och friheter enligt denna förordning. Skyddsåtgärderna bör säkerställa att tekniska och organisatoriska åtgärder har införts för att se till att särskilt principen om uppgiftsminimering iakttas. Ytterligare behandling av personuppgifter för arkivändamål av allmänintresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör genomföras, när den personuppgiftsansvarige har bedömt möjligheten att uppnå dessa ändamål genom behandling av personuppgifter som inte medger eller inte längre medger identifiering av de registrerade, förutsatt att det finns lämpliga skyddsåtgärder (t. ex. pseudonymisering av personuppgifter). Medlemsstaterna bör införa lämpliga skyddsåtgärder för behandlingen av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Medlemsstaterna bör på särskilda villkor med förbehåll för lämpliga skyddsåtgärder för de registrerade ha rätt att specificera och göra undantag från kraven på information, rätten till rättelse eller radering av personuppgifter, rätten att bli bortglömd, rätten till begränsning av behandlingen, rätten till dataportabilitet och rätten att göra invändning i samband med behandling av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Villkoren och säkerhetsåtgärderna i fråga kan medföra att de registrerade måste följa särskilda förfaranden för att utöva dessa rättigheter, om det är lämpligt med hänsyn till den särskilda behandlingens syfte tillsammans med tekniska och organisatoriska åtgärder som syftar till att minimera behandlingen av personuppgifter i enlighet med principerna om proportionalitet och nödvändighet. Behandling av personuppgifter för vetenskapliga ändamål bör även vara förenlig med annan relevant lagstiftning, exempelvis om kliniska prövningar.
- (157) Genom att koppla samman information från olika register kan forskare erhålla ny kunskap av stort värde med avseende på medicinska tillstånd som exempelvis hjärt-kärlsjukdomar, cancer och depression. På grundval av registren kan forskningsresultaten förbättras, eftersom de bygger på en större befolkningsgrupp. Forskning inom samhällsvetenskap som bedrivs på grundval av register gör det möjligt för forskare att få grundläggande kunskaper om sambandet på lång sikt mellan ett antal sociala villkor, exempelvis arbetslöshet och utbildning, och andra livsförhållanden. Forskningsresultat som erhållits på grundval av register utgör en stabil, högkvalitativ kunskap, som kan ligga till grund för utformningen och genomförandet av kunskapsbaserad politik, förbättra livskvaliteten för ett antal personer och förbättra de sociala tjänsternas effektivitet. För att underlätta vetenskaplig forskning får personuppgifter behandlas för vetenskapliga forskningsändamål, med förbehåll för lämpliga villkor och skyddsåtgärder i unionsrätten eller i medlemsstaternas nationella rätt.
- (158) Om personuppgifter behandlas för arkivändamål, bör denna förordning också gälla denna behandling, med beaktande av att denna förordning inte bör gälla för avlidna personer. Offentliga myndigheter eller offentliga eller privata organ som innehar uppgifter av allmänt intresse bör vara tillhandahållare som, i enlighet med unionsrätten eller medlemsstaternas nationella rätt, har en rättslig skyldighet att förvärva, bevara, bedöma, organisera, beskriva, kommunicera, främja, sprida och ge tillgång till uppgifter av bestående värde för allmänintresset. Medlemsstaterna bör också ha rätt att föreskriva att personuppgifter får vidarebehandlas för arkivering, exempelvis i syfte att tillhandahålla specifik information om politiskt beteende under tidigare totalitära regimer, folkmord, brott mot mänskligheten, särskilt Förintelsen, eller krigsförbrytelser.

- (159) Om personuppgifter behandlas för vetenskapliga forskningsändamål, bör denna förordning också gälla denna behandling. Behandling av personuppgifter för vetenskapliga forskningsändamål bör i denna förordning ges en vid tolkning och omfatta till exempel teknisk utveckling och demonstration, grundforskning, tillämpad forskning och privatfinansierad forskning. Behandlingen av personuppgifter bör dessutom ta hänsyn till unionens mål enligt artikel 179.1 i EUF-fördraget angående åstadkommandet av ett europeiskt forskningsområde. Vetenskapliga forskningsändamål bör också omfatta studier som utförs av ett allmänt intresse inom folkhälsoområdet. För att tillgodose de särskilda kraven i samband med behandling av personuppgifter för vetenskapliga forskningsändamål bör särskilda villkor gälla, särskilt vad avser offentliggörande eller annat utlämnande av personuppgifter inom ramen för vetenskapliga forskningsändamål. Om resultatet av vetenskaplig forskning, särskilt för hälso- och sjukvårdsändamål, ger anledning till ytterligare åtgärder i den registrerades intresse, bör de allmänna reglerna i denna förordning tillämpas på dessa åtgärder.
- (160) Om personuppgifter behandlas för historiska forskningsändamål, bör denna förordning också gälla denna behandling. Detta bör även omfatta forskning för historiska och genealogiska ändamål, med beaktande av att denna förordning inte bör gälla för avlidna personer.
- (161) När det gäller samtycke till deltagande i vetenskaplig forskning inom ramen för kliniska prövningar, bör de relevanta bestämmelserna i Europaparlamentets och rådets förordning (EU) nr 536/2014 ⁽¹⁾ tillämpas.
- (162) Om personuppgifter behandlas för statistiska ändamål, bör denna förordning gälla denna behandling. Unionsrätten eller medlemsstaternas nationella rätt bör, inom ramen för denna förordning, fastställa statistiskt innehåll, kontroll av tillgång, specifikationer för behandling av personuppgifter för statistiska ändamål och lämpliga åtgärder till skydd för den registrerades rättigheter och friheter och för att säkerställa insynsskydd för statistiska uppgifter. Med statistiska ändamål avses varje åtgärd som vidtas för den insamling och behandling av personuppgifter som är nödvändig för statistiska undersökningar eller för framställning av statistiska resultat. Dessa statistiska resultat kan vidare användas för olika ändamål, inbegripet vetenskapliga forskningsändamål. Ett statistiskt ändamål innebär att resultatet av behandlingen för statistiska ändamål inte består av personuppgifter, utan av aggregerade personuppgifter, och att resultatet eller uppgifterna inte används till stöd för åtgärder eller beslut som avser en särskild fysiskperson.
- (163) De konfidentiella uppgifter som unionens myndigheter och nationella statistikansvariga myndigheter samlar in för att framställa officiell europeisk och officiell nationell statistik bör skyddas. Europeisk statistik bör utvecklas, framställas och spridas i enlighet med de statistiska principerna i artikel 338.2 i EUF-fördraget, medan hanteringen av nationell statistik även bör överensstämma med medlemsstaternas nationella rätt. Europaparlamentets och rådets förordning (EG) nr 223/2009 ⁽²⁾ innehåller ytterligare preciseringar om statistisk konfidentialitet för europeisk statistik.
- (164) Vad beträffar tillsynsmyndigheternas befogenheter att från personuppgiftsansvariga eller personuppgiftsbiträden få tillgång till personuppgifter och tillträde till lokaler, får medlemsstaterna, inom gränserna för denna förordning, genom lagstiftning anta särskilda regler för att skydda yrkesmässig eller annan motsvarande tystnadsplikt, i den mån detta är nödvändigt för att jämka samman rätten till skydd av personuppgifter med tystnadsplikten. Detta påverkar inte tillämpningen av medlemsstaternas befintliga skyldigheter att anta bestämmelser om tystnadsplikt, där detta krävs enligt unionsrätten.
- (165) Denna förordning är förenlig med kravet på att respektera och inte påverka den ställning som kyrkor och religiösa sammanslutningar eller samfund har i medlemsstaterna enligt gällande grundlag i enlighet med artikel 17 i EUF-fördraget.
- (166) I syfte att uppnå målen för denna förordning, nämligen att skydda fysiska personers grundläggande rättigheter och friheter och i synnerhet deras rätt till skydd av personuppgifter och för att säkra det fria flödet av

⁽¹⁾ Europaparlamentets och rådets förordning (EU) nr 536/2014 av den 16 april 2014 om kliniska prövningar av humanläkemedel och om upphävande av direktiv 2001/20/EG (EUT L 158, 27.5.2014, s. 1).

⁽²⁾ Europaparlamentets och rådets förordning (EG) nr 223/2009 av den 11 mars 2009 om europeisk statistik och om upphävande av Europaparlamentets och rådets förordning (EG, Euratom) nr 1101/2008 om utlämnande av insynsskyddade statistiska uppgifter till Europeiska gemenskapernas statistikkontor, rådets förordning (EG) nr 322/97 om gemenskapsstatistik och rådets beslut 89/382/EEG, Euratom om inrättande av en kommitté för Europeiska gemenskapernas statistiska program (EUT L 87, 31.3.2009, s. 164).

personuppgifter inom unionen, bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen. Delegerade akter bör framför allt antas när det gäller kriterier och krav vad gäller certifieringsmekanismer, information som ska ges med användning av standardiserade symboler och förfaranden för att tillhandahålla sådana symboler. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå. När kommissionen förbereder och utarbetar delegerade akter bör den se till att relevanta handlingar översänds samtidigt till Europaparlamentet och rådet och att detta sker så snabbt som möjligt och på lämpligt sätt.

- (167) För att säkerställa enhetliga villkor för tillämpningen av denna förordning bör kommissionen ges genomförande-befogenheter i enlighet med denna förordning. Dessa befogenheter bör utövas i enlighet med förordning (EU) nr 182/2011. Kommissionen bör därvid överväga särskilda åtgärder för mikroföretag och små och medelstora företag.
- (168) Granskningsförfarandet bör användas vid antagande av genomförandeakter om standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden och mellan personuppgiftsbiträden, uppförandekoder, tekniska standarder och mekanismer för certifiering, adekvat nivå på det skydd som lämnas av ett tredjeland, ett territorium eller av en specificerad sektor inom det tredjelandet eller en internationell organisation, standardiserade skyddsbestämmelser, format och förfaranden för elektroniskt utbyte av information mellan personuppgiftsansvariga, personuppgiftsbiträden och tillsynsmyndigheter för bindande företagsbestämmelser, ömsesidigt bistånd och tillvägagångssätt för elektroniskt utbyte av information mellan tillsynsmyndigheter samt mellan tillsynsmyndigheter och styrelsen.
- (169) Kommissionen bör när det föreligger tvingande skäl till skyndsamt anta omedelbart tillämpliga genomförandeakter, när tillgängliga bevis visar att ett tredjeland, ett territorium eller en specificerad sektor inom det tredjelandet eller en internationell organisation inte upprätthåller en adekvat skyddsnivå.
- (170) Eftersom målet för denna förordning, nämligen att säkerställa en likvärdig nivå för skyddet av fysiska personer och det fria flödet av personuppgifter inom hela unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens omfattning eller verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen (EU-fördraget). I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.
- (171) Direktiv 95/46/EG bör upphävas genom denna förordning. Behandling som redan pågår den dag då denna förordning börjar tillämpas bör bringas i överensstämmelse med denna förordning inom en period av två år från det att denna förordning träder i kraft. Om behandlingen grundar sig på samtycke enligt direktiv 95/46/EG, är det inte nödvändigt att den registrerade på nytt ger sitt samtycke för att den personuppgiftsansvarige ska kunna fortsätta med behandlingen i fråga efter det att denna förordning börjar tillämpas, om det sätt på vilket samtycket gavs överensstämmer med villkoren i denna förordning. Beslut av kommissionen som antagits och tillstånd från tillsynsmyndigheterna som utfärdats på grundval av direktiv 95/46/EG ska fortsatt vara giltiga tills de ändras, ersätts eller upphävs.
- (172) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i förordning (EG) nr 45/2001 och avgav ett yttrande den 7 mars 2012 ⁽¹⁾.
- (173) Denna förordning bör vara tillämplig på alla frågor som gäller skyddet av grundläggande rättigheter och friheter i förhållande till behandlingen av personuppgifter, vilka inte omfattas av särskilda skyldigheter med samma mål som anges i Europaparlamentets och rådets direktiv 2002/58/EG ⁽²⁾, däribland den personuppgiftsansvariges skyldigheter och fysiska personers rättigheter. För att klargöra förhållandet mellan denna förordning och direktiv 2002/58/EG bör det direktivet ändras. När denna förordning har antagits, bör direktiv 2002/58/EG ses över, framför allt för att säkerställa konsekvens med denna förordning.

⁽¹⁾ EUT C 192, 30.6.2012, s. 7.

⁽²⁾ Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Allmänna bestämmelser

Artikel 1

Syfte

1. I denna förordning fastställs bestämmelser om skydd för fysiska personer med avseende på behandlingen av personuppgifter och om det fria flödet av personuppgifter.
2. Denna förordning skyddar fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.
3. Det fria flödet av personuppgifter inom unionen får varken begränsas eller förbjudas av skäl som rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter.

Artikel 2

Materiellt tillämpningsområde

1. Denna förordning ska tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.
2. Denna förordning ska inte tillämpas på behandling av personuppgifter som
 - a) utgör ett led i en verksamhet som inte omfattas av unionsrätten,
 - b) medlemsstaterna utför när de bedriver verksamhet som omfattas av avdelning V kapitel 2 i EU-fördraget,
 - c) en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll,
 - d) behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.
3. Förordning (EG) nr 45/2001 är tillämplig på den behandling av personuppgifter som sker i EU:s institutioner, organ och byråer. Förordning (EG) nr 45/2001 och de av unionens övriga rättsakter som är tillämpliga på sådan behandling av personuppgifter ska anpassas till principerna och bestämmelserna i denna förordning i enlighet med artikel 98.
4. Denna förordning påverkar inte tillämpningen av direktiv 2000/31/EG, särskilt bestämmelserna om tjänstelevererande mellanhänders ansvar i artiklarna 12–15 i det direktivet.

Artikel 3

Territoriellt tillämpningsområde

1. Denna förordning ska tillämpas på behandlingen av personuppgifter inom ramen för den verksamhet som bedrivs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad i unionen, oavsett om behandlingen utförs i unionen eller inte.

2. Denna förordning ska tillämpas på behandling av personuppgifter som avser registrerade som befinner sig i unionen och som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad i unionen, om behandlingen har anknytning till

- a) utbudande av varor eller tjänster till sådana registrerade i unionen, oavsett om dessa varor eller tjänster erbjuds kostnadsfritt eller inte, eller
- b) övervakning av deras beteende så länge beteendet sker inom unionen.

3. Denna förordning ska tillämpas på behandling av personuppgifter som utförs av en personuppgiftsansvarig som inte är etablerad i unionen, men på en plats där en medlemsstats nationella rätt gäller enligt folkrätten.

Artikel 4

Definitioner

I denna förordning avses med

1. *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad *en registrerad*), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,
2. *behandling*: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring,
3. *begränsning av behandling*: markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden,
4. *profilering*: varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar,
5. *pseudonymisering*: behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person,
6. *register*: en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden,
7. *personuppgiftsansvarig*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt,
8. *personuppgiftsbiträde*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,
9. *mottagare*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilket personuppgifterna utlämnas, vare sig det är en tredje part eller inte; offentliga myndigheter som kan komma att motta

personuppgifter inom ramen för ett särskilt uppdrag i enlighet med unionsrätten eller medlemsstaternas nationella rätt ska dock inte betraktas som mottagare; offentliga myndigheters behandling av dessa uppgifter ska vara förenlig med tillämpliga bestämmelser för dataskydd beroende på behandlingens syfte,

10. *tredje part*: en fysisk eller juridisk person, offentlig myndighet, institution eller organ som inte är den registrerade, den personuppgiftsansvarige, personuppgiftsbiträdet eller de personer som under den personuppgiftsansvariges eller personuppgiftsbitrådets direkta ansvar är behöriga att behandla personuppgifterna,
11. *samtycke* av den registrerade: varje slag av frivillig, specifik, informerad och otvetydig viljeytring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne,
12. *personuppgiftsincident*: en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats,
13. *genetiska uppgifter*: alla personuppgifter som rör nedärvda eller förvärvade genetiska kännetecken för en fysisk person, vilka ger unik information om denna fysiska persons fysiologi eller hälsa och vilka framför allt härrör från en analys av ett biologiskt prov från den fysiska personen i fråga,
14. *biometriska uppgifter*: personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter,
15. *uppgifter om hälsa*: personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus,
16. *huvudsakligt verksamhetsställe*:
 - a) när det gäller en personuppgiftsansvarig med verksamhetsställen i mer än en medlemsstat, den plats i unionen där vederbörande har sin centrala förvaltning, om inte besluten om ändamålen och medlen för behandlingen av personuppgifter fattas vid ett annat av den personuppgiftsansvariges verksamhetsställen i unionen och det sistnämnda verksamhetsstället har befogenhet att få sådana beslut genomförda, i vilket fall det verksamhetsställe som har fattat sådana beslut ska betraktas som det huvudsakliga verksamhetsstället,
 - b) när det gäller ett personuppgiftsbiträde med verksamhetsställen i mer än en medlemsstat, den plats i unionen där vederbörande har sin centrala förvaltning eller, om personuppgiftsbiträdet inte har någon central förvaltning i unionen, det av personuppgiftsbitrådets verksamhetsställen i unionen där den huvudsakliga behandlingen inom ramen för verksamheten vid ett av personuppgiftsbitrådets verksamhetsställen sker, i den utsträckning som personuppgiftsbiträdet omfattas av särskilda skyldigheter enligt denna förordning,
17. *företrädare*: en i unionen etablerad fysisk eller juridisk person som skriftligen har utsetts av den personuppgiftsansvarige eller personuppgiftsbiträdet i enlighet med artikel 27 och företräder denne i frågor som gäller dennes skyldigheter enligt denna förordning,
18. *företag*: en fysisk eller juridisk person som bedriver ekonomisk verksamhet, oavsett dess juridiska form, vilket inbegriper partnerskap eller föreningar som regelbundet bedriver ekonomisk verksamhet,
19. *koncern*: ett kontrollerande företag och dess kontrollerade företag,
20. *bindande företagsbestämmelser*: strategier för skydd av personuppgifter som en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad på en medlemsstats territorium använder sig av vid överföringar eller en uppsättning av överföringar av personuppgifter till en personuppgiftsansvarig eller ett personuppgiftsbiträde i ett eller flera tredjeländer inom en koncern eller en grupp av företag som deltar i gemensam ekonomisk verksamhet,
21. *tillsynsmyndighet*: en oberoende offentlig myndighet som är utsedd av en medlemsstat i enlighet med artikel 51,

22. *berörd tillsynsmyndighet*: en tillsynsmyndighet som berörs av behandlingen av personuppgifter på grund av att
- den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad på tillsynsmyndighetens medlemsstats territorium,
 - registrerade som är bosatta i den tillsynsmyndighetens medlemsstat i väsentlig grad påverkas eller sannolikt i väsentlig grad kommer att påverkas av behandlingen, eller
 - ett klagomål har lämnats in till denna tillsynsmyndighet,
23. *gränsöverskridande behandling*:
- behandling av personuppgifter som äger rum inom ramen för verksamhet vid verksamhetsställen i mer än en medlemsstat tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen, när den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad i mer än en medlemsstat, eller
 - behandling av personuppgifter som äger rum inom ramen för verksamhet vid ett enda verksamhetsställe tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen men som i väsentlig grad påverkar eller sannolikt i väsentlig grad kommer att påverka registrerade i mer än en medlemsstat,
24. *relevant och motiverad invändning*: en invändning mot ett förslag till beslut avseende frågan huruvida det föreligger en överträdelse av denna förordning eller huruvida den planerade åtgärden i förhållande till den personuppgiftsansvarige eller personuppgiftsbiträdet är förenlig med denna förordning, av vilken invändning det tydligt framgår hur stora risker utkastet till beslut medför när det gäller registrerades grundläggande rättigheter och friheter samt i tillämpliga fall det fria flödet av personuppgifter inom unionen,
25. *informationssamhällets tjänster*: alla tjänster enligt definitionen i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535 ⁽¹⁾,
26. *internationell organisation*: en organisation och dess underställda organ som lyder under folkrätten, eller ett annat organ som inrättats genom eller på grundval av en överenskommelse mellan två eller flera länder.

KAPITEL II

Principer

Artikel 5

Principer för behandling av personuppgifter

- Vid behandling av personuppgifter ska följande gälla:
 - Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (*laglighet, korrekthet och öppenhet*).
 - De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska inte anses vara oförenligt med de ursprungliga ändamålen (*ändamålsbegränsning*).
 - De ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (*uppgiftsminimering*).
 - De ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål (*korrekthet*).

⁽¹⁾ Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (EUT L 241, 17.9.2015, s. 1).

- e) De får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, under förutsättning att de lämpliga tekniska och organisatoriska åtgärder som krävs enligt denna förordning genomförs för att säkerställa den registrerades rättigheter och friheter (*lagringsminimering*).
 - f) De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstörelse eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (*integritet och konfidentialitet*).
2. Den personuppgiftsansvarige ska ansvara för och kunna visa att punkt 1 efterlevs (*ansvarsskyldighet*).

Artikel 6

Laglig behandling av personuppgifter

1. Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:
- a) Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.
 - b) Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.
 - c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.
 - d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.
 - e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.
 - f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

Led f i första stycket ska inte gälla för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter.

2. Medlemsstaterna får behålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i denna förordning med hänsyn till behandling för att efterleva punkt 1 c och e genom att närmare fastställa specifika krav för uppgiftsbehandlingen och andra åtgärder för att säkerställa en laglig och rättvis behandling, inbegripet för andra specifika situationer då uppgifter behandlas i enlighet med kapitel IX.

3. Den grund för behandlingen som avses i punkt 1 c och e ska fastställas i enlighet med

- a) unionsrätten, eller
- b) en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av.

Syftet med behandlingen ska fastställas i den rättsliga grunden eller, i fråga om behandling enligt punkt 1 e, ska vara nödvändigt för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Den rättsliga grunden kan innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i denna förordning, bland annat: de allmänna villkor som ska gälla för den personuppgiftsansvariges behandling, vilken typ av uppgifter som ska behandlas, vilka registrerade som berörs, de enheter till vilka personuppgifterna får lämnas ut och för vilka ändamål, ändamålsbegränsningar, lagringstid samt typer av behandling och förfaranden för behandling, inbegripet åtgärder för att tillförsäkra en laglig och rättvis behandling, däribland för behandling i andra särskilda

situationer enligt kapitel IX. Unionsrätten eller medlemsstaternas nationella rätt ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas.

4. Om en behandling för andra ändamål än det ändamål för vilket personuppgifterna samlades in inte grundar sig på den registrerades samtycke eller på unionsrätten eller medlemsstaternas nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda de mål som avses i artikel 23.1, ska den personuppgiftsansvarige för att fastställa huruvida behandling för andra ändamål är förenlig med det ändamål för vilket personuppgifterna ursprungligen samlades in bland annat beakta följande:

- a) Kopplingar mellan de ändamål för vilka personuppgifterna har samlats in och ändamålen med den avsedda ytterligare behandlingen.
- b) Det sammanhang inom vilket personuppgifterna har samlats in, särskilt förhållandet mellan de registrerade och den personuppgiftsansvarige.
- c) Personuppgifternas art, särskilt huruvida särskilda kategorier av personuppgifter behandlas i enlighet med artikel 9 eller huruvida personuppgifter om fällande domar i brottmål och överträdelse behandlas i enlighet med artikel 10.
- d) Eventuella konsekvenser för registrerade av den planerade fortsatta behandlingen.
- e) Förekomsten av lämpliga skyddsåtgärder, vilket kan inbegripa kryptering eller pseudonymisering.

Artikel 7

Villkor för samtycke

1. Om behandlingen grundar sig på samtycke, ska den personuppgiftsansvarige kunna visa att den registrerade har samtyckt till behandling av sina personuppgifter.
2. Om den registrerades samtycke lämnas i en skriftlig förklaring som också rör andra frågor, ska begäran om samtycke läggas fram på ett sätt som klart och tydligt kan särskiljas från de andra frågorna i en begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. Om en del av förklaringen innebär en överträdelse av denna förordning, ska denna del inte vara bindande.
3. De registrerade ska ha rätt att när som helst återkalla sitt samtycke. Återkallandet av samtycket ska inte påverka lagligheten av behandling som grundar sig på samtycke, innan detta återkallas. Innan samtycke lämnas ska den registrerade informeras om detta. Det ska vara lika lätt att återkalla som att ge sitt samtycke.
4. Vid bedömning av huruvida samtycke är frivilligt ska största hänsyn bland annat tas till huruvida genomförandet av ett avtal, inbegripet tillhandahållandet av en tjänst, har gjorts beroende av samtycke till sådan behandling av personuppgifter som inte är nödvändig för genomförandet av det avtalet.

Artikel 8

Villkor som gäller barns samtycke avseende informationssamhällets tjänster

1. Vid erbjudande av informationssamhällets tjänster direkt till ett barn, ska vid tillämpningen av artikel 6.1 a behandling av personuppgifter som rör ett barn vara tillåten om barnet är minst 16 år. Om barnet är under 16 år ska sådan behandling vara tillåten endast om och i den mån samtycke ges eller godkänns av den person som har föräldrans ansvar för barnet.

Medlemsstaterna får i sin nationella rätt föreskriva en lägre ålder i detta syfte, under förutsättning att denna lägre ålder inte är under 13 år.

2. Den personuppgiftsansvarige ska göra rimliga ansträngningar för att i sådana fall kontrollera att samtycke ges eller godkänns av den person som har föräldraansvar för barnet, med hänsyn tagen till tillgänglig teknik.
3. Punkt 1 ska inte påverka tillämpningen av allmän avtalsrätt i medlemsstaterna, såsom bestämmelser om giltigheten, upprättandet eller effekten av ett avtal som gäller ett barn.

Artikel 9

Behandling av särskilda kategorier av personuppgifter

1. Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning ska vara förbjuden.
2. Punkt 1 ska inte tillämpas om något av följande gäller:
 - a) Den registrerade har uttryckligen lämnat sitt samtycke till behandlingen av dessa personuppgifter för ett eller flera specifika ändamål, utom då unionsrätten eller medlemsstaternas nationella rätt föreskriver att förbudet i punkt 1 inte kan upphävas av den registrerade.
 - b) Behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och på områdena social trygghet och socialt skydd, i den omfattning detta är tillåtet enligt unionsrätten eller medlemsstaternas nationella rätt eller ett kollektivavtal som antagits med stöd av medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder som säkerställer den registrerades grundläggande rättigheter och intressen fastställs.
 - c) Behandlingen är nödvändig för att skydda den registrerades eller någon annan fysisk persons grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.
 - d) Behandlingen utförs inom ramen för berättigad verksamhet med lämpliga skyddsåtgärder hos en stiftelse, en förening eller ett annat icke vinstdrivande organ, som har ett politiskt, filosofiskt, religiöst eller fackligt syfte, förutsatt att behandlingen enbart rör sådana organs medlemmar eller tidigare medlemmar eller personer som på grund av organets ändamål har regelbunden kontakt med detta och personuppgifterna inte lämnas ut utanför det organet utan den registrerades samtycke.
 - e) Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.
 - f) Behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk eller som en del av domstolarnas dömande verksamhet.
 - g) Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.
 - h) Behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård, behandling, social omsorg eller förvaltning av hälso- och sjukvårdstjänster och social omsorg och av deras system, på grundval av unionsrätten eller medlemsstaternas nationella rätt eller enligt avtal med yrkesverksamma på hälsoområdet och under förutsättning att de villkor och skyddsåtgärder som avses i punkt 3 är uppfyllda.
 - i) Behandlingen är nödvändig av skäl av allmänt intresse på folkhälsoområdet, såsom behovet av att säkerställa ett skydd mot allvarliga gränsöverskridande hot mot hälsan eller säkerställa höga kvalitets- och säkerhetsnormer för vård och läkemedel eller medicintekniska produkter, på grundval av unionsrätten eller medlemsstaternas nationella rätt, där lämpliga och specifika åtgärder för att skydda den registrerades rättigheter och friheter fastställs, särskilt tystnadsplikt.

- j) Behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.
3. Personuppgifter som avses i punkt 1 får behandlas för de ändamål som avses i punkt 2 h, när uppgifterna behandlas av eller under ansvar av en yrkesutövare som omfattas av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställs av nationella behöriga organ eller av en annan person som också omfattas av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställs av nationella behöriga organ.
4. Medlemsstaterna får behålla eller införa ytterligare villkor, även begränsningar, för behandlingen av genetiska eller biometriska uppgifter eller uppgifter om hälsa.

Artikel 10

Behandling av personuppgifter som rör fällande domar i brottmål samt överträdelser

Behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder enligt artikel 6.1 får endast utföras under kontroll av myndighet eller då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs. Ett fullständigt register över fällande domar i brottmål får endast föras under kontroll av en myndighet.

Artikel 11

Behandling som inte kräver identifiering

1. Om de ändamål för vilka den personuppgiftsansvarige behandlar personuppgifter inte kräver eller inte längre kräver att den registrerade identifieras av den personuppgiftsansvarige, ska den personuppgiftsansvarige inte vara tvungen att bevara, förvärva eller behandla ytterligare information för att identifiera den registrerade endast i syfte att följa denna förordning.
2. Om den personuppgiftsansvarige, i de fall som avses i punkt 1 i denna artikel, kan visa att denne inte är i stånd att identifiera den registrerade, ska den personuppgiftsansvarige om möjligt informera den registrerade om detta. I sådana fall ska artiklarna 15–20 inte gälla, förutom när den registrerade för utövande av sina rättigheter i enlighet med dessa artiklar tillhandahåller ytterligare information som gör identifieringen möjlig.

KAPITEL III

Den registrerades rättigheter

Avsnitt 1

Insyn och villkor

Artikel 12

Klar och tydlig information och kommunikation samt klara och tydliga villkor för utövandet av den registrerades rättigheter

1. Den personuppgiftsansvarige ska vidta lämpliga åtgärder för att till den registrerade tillhandahålla all information som avses i artiklarna 13 och 14 och all kommunikation enligt artiklarna 15–22 och 34 vilken avser behandling i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, i synnerhet för information som är särskilt riktad till barn. Informationen ska tillhandahållas skriftligt, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form. Om den registrerade begär det får informationen tillhandahållas muntligt, förutsatt att den registrerades identitet bevisats på andra sätt.

2. Den personuppgiftsansvarige ska underlätta utövandet av den registrerades rättigheter i enlighet med artiklarna 15–22. I de fall som avses i artikel 11.2 får den personuppgiftsansvarige inte vägra att tillmötesgå den registrerades begäran om att utöva sina rättigheter enligt artiklarna 15–22, om inte den personuppgiftsansvarige visar att han eller hon inte är i stånd att identifiera den registrerade.

3. Den personuppgiftsansvarige ska på begäran utan onödigt dröjsmål och under alla omständigheter senast en månad efter att ha mottagit begäran tillhandahålla den registrerade information om de åtgärder som vidtagits enligt artiklarna 15–22. Denna period får vid behov förlängas med ytterligare två månader, med beaktande av hur komplicerad begäran är och antalet inkomna begäranden. Den personuppgiftsansvarige ska underrätta den registrerade om en sådan förlängning inom en månad från det att begäran mottagits samt ange orsakerna till förseningen. Om den registrerade lämnar begäran i elektronisk form, ska informationen om möjligt tillhandahållas i elektronisk form, om den registrerade inte begär något annat.

4. Om den personuppgiftsansvarige inte vidtar åtgärder på den registrerades begäran, ska den personuppgiftsansvarige utan dröjsmål och senast en månad efter att ha mottagit begäran informera den registrerade om orsaken till att åtgärder inte vidtagits och om möjligheten att lämna in ett klagomål till en tillsynsmyndighet och begära rättslig prövning.

5. Information som tillhandahållits enligt artiklarna 13 och 14, all kommunikation och samtliga åtgärder som vidtas enligt artiklarna 15–22 och 34 ska tillhandahållas kostnadsfritt. Om begäranden från en registrerad är uppenbart ogrundade eller orimliga, särskilt på grund av deras repetitiva art, får den personuppgiftsansvarige antingen

- a) ta ut en rimlig avgift som täcker de administrativa kostnaderna för att tillhandahålla den information eller vidta den åtgärd som begärts, eller
- b) vägra att tillmötesgå begäran.

Det åligger den personuppgiftsansvarige att visa att begäran är uppenbart ogrundad eller orimlig.

6. Utan att det påverkar tillämpningen av artikel 11 får den personuppgiftsansvarige, om denne har rimliga skäl att betvivla identiteten hos den fysiska person som lämnar in en begäran enligt artiklarna 15–21, begära att ytterligare information som är nödvändig för att bekräfta den registrerades identitet tillhandahålls.

7. Den information som ska tillhandahållas de registrerade i enlighet med artiklarna 13 och 14 får tillhandahållas kombinerad med standardiserade symboler för att ge en överskådlig, begriplig, lättläst och meningsfull överblick över den planerade behandlingen. Om sådana symboler visas elektroniskt ska de vara maskinläsbara.

8. Kommissionen ska ges befogenhet att anta delegerade akter i enlighet med artikel 92 för att fastställa vilken information som ska visas med hjälp av symboler och förfaranden för att tillhandahålla sådana symboler.

Avsnitt 2

Information och tillgång till personuppgifter

Artikel 13

Information som ska tillhandahållas om personuppgifterna samlas in från den registrerade

1. Om personuppgifter som rör en registrerad person samlas in från den registrerade, ska den personuppgiftsansvarige, när personuppgifterna erhålls, till den registrerade lämna information om följande:

- a) Identitet och kontaktuppgifter för den personuppgiftsansvarige och i tillämpliga fall för dennes företrädare.
- b) Kontaktuppgifter för dataskyddsombudet, i tillämpliga fall.
- c) Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen.

- d) Om behandlingen är baserad på artikel 6.1 f, den personuppgiftsansvariges eller en tredje parts berättigade intressen.
- e) Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall.
- f) I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artikel 46, 47 eller artikel 49.1 andra stycket, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.
2. Utöver den information som avses i punkt 1 ska den personuppgiftsansvarige vid insamlingen av personuppgifterna lämna den registrerade följande ytterligare information, vilken krävs för att säkerställa rättvis och transparent behandling:
- a) Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.
- b) Att det föreligger en rätt att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller att invända mot behandling samt rätten till dataportabilitet.
- c) Om behandlingen grundar sig på artikel 6.1 a eller artikel 9.2 a, att det föreligger en rätt att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.
- d) Rätten att inge klagomål till en tillsynsmyndighet.
- e) Huruvida tillhandahållandet av personuppgifter är ett lagstadgat eller avtalsenligt krav eller ett krav som är nödvändigt för att ingå ett avtal samt huruvida den registrerade är skyldig att tillhandahålla personuppgifterna och de möjliga följderna av att sådana uppgifter inte lämnas.
- f) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.
3. Om den personuppgiftsansvarige avser att ytterligare behandla personuppgifterna för ett annat syfte än det för vilket de insamlades, ska den personuppgiftsansvarige före denna ytterligare behandling ge den registrerade information om detta andra syfte samt ytterligare relevant information enligt punkt 2.
4. Punkterna 1, 2 och 3 ska inte tillämpas om och i den mån den registrerade redan förfogar över informationen.

Artikel 14

Information som ska tillhandahållas om personuppgifterna inte har erhållits från den registrerade

1. Om personuppgifterna inte har erhållits från den registrerade, ska den personuppgiftsansvarige förse den registrerade med följande information:
- a) Identitet och kontaktuppgifter för den personuppgiftsansvarige och i tillämpliga fall för dennes företrädare.
- b) Kontaktuppgifter för dataskyddsombudet, i tillämpliga fall.
- c) Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen.
- d) De kategorier av personuppgifter som behandlingen gäller.
- e) Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall.

- f) I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till en mottagare i ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artiklarna 46, 47 eller artikel 49.1 andra stycket, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.
2. Utöver den information som avses i punkt 1 ska den personuppgiftsansvarige lämna den registrerade följande information, vilken krävs för att säkerställa rättvis och transparent behandling när det gäller den registrerade:
- a) Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.
 - b) Om behandlingen grundar sig på artikel 6.1 f, den personuppgiftsansvariges eller en tredje parts berättigade intressen.
 - c) Förekomsten av rätten att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade och att invända mot behandling samt rätten till dataportabilitet.
 - d) Om behandlingen grundar sig på artikel 6.1 a eller artikel 9.2 a, rätten att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.
 - e) Rätten att inge klagomål till en tillsynsmyndighet.
 - f) Varifrån personuppgifterna kommer och i förekommande fall huruvida de har sitt ursprung i allmänt tillgängliga källor.
 - g) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.
3. Den personuppgiftsansvarige ska lämna den information som anges i punkterna 1 och 2
- a) inom en rimlig period efter det att personuppgifterna har erhållits, dock senast inom en månad, med beaktande av de särskilda omständigheter under vilka personuppgifterna behandlas,
 - b) om personuppgifterna ska användas för kommunikation med den registrerade, senast vid tidpunkten för den första kommunikationen med den registrerade, eller
 - c) om ett utlämnande till en annan mottagare förutses, senast när personuppgifterna lämnas ut för första gången.
4. Om den personuppgiftsansvarige avser att ytterligare behandla personuppgifterna för ett annat syfte än det för vilket de insamlades, ska den personuppgiftsansvarige före denna ytterligare behandling ge den registrerade information om detta andra syfte samt ytterligare relevant information enligt punkt 2.
5. Punkterna 1–4 ska inte tillämpas i följande fall och i den mån
- a) den registrerade redan förfogar över informationen,
 - b) tillhandahållandet av sådan information visar sig vara omöjligt eller skulle medföra en oproportionell ansträngning, särskilt för behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, eller i den mån den skyldighet som avses i punkt 1 i den här artikeln sannolikt kommer att göra det omöjligt eller avsevärt försvårar uppfyllandet av målen med den behandlingen; i sådana fall ska den personuppgiftsansvarige vidta lämpliga åtgärder för att skydda den registrerades rättigheter och friheter och berättigade intressen, inbegripet göra uppgifterna tillgängliga för allmänheten,
 - c) erhållande eller utlämnande av uppgifter uttryckligen föreskrivs genom unionsrätten eller genom en medlemsstats nationella rätt som den registrerade omfattas av och som fastställer lämpliga åtgärder för att skydda den registrerades berättigade intressen, eller
 - d) personuppgifterna måste förbli konfidentiella till följd av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt, inbegripet andra lagstadgade sekretessförpliktelser.

*Artikel 15***Den registrerades rätt till tillgång**

1. Den registrerade ska ha rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna och följande information:
 - a) Ändamålen med behandlingen.
 - b) De kategorier av personuppgifter som behandlingen gäller.
 - c) De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, särskilt mottagare i tredjeländer eller internationella organisationer.
 - d) Om möjligt, den förutsedda period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.
 - e) Förekomsten av rätten att av den personuppgiftsansvarige begära rättelse eller radering av personuppgifterna eller begränsning av behandling av personuppgifter som rör den registrerade eller att invända mot sådan behandling.
 - f) Rätten att inge klagomål till en tillsynsmyndighet.
 - g) Om personuppgifterna inte samlas in från den registrerade, all tillgänglig information om varifrån dessa uppgifter kommer.
 - h) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.
2. Om personuppgifterna överförs till ett tredjeland eller till en internationell organisation, ska den registrerade ha rätt till information om de lämpliga skyddsåtgärder som i enlighet med artikel 46 har vidtagits vid överföringen.
3. Den personuppgiftsansvarige ska förse den registrerade med en kopia av de personuppgifter som är under behandling. För eventuella ytterligare kopior som den registrerade begär får den personuppgiftsansvarige ta ut en rimlig avgift på grundval av de administrativa kostnaderna. Om den registrerade gör begäran i elektronisk form ska informationen tillhandahållas i ett elektroniskt format som är allmänt använt, om den registrerade inte begär något annat.
4. Den rätt till en kopia som avses i punkt 3 ska inte inverka menligt på andras rättigheter och friheter.

*Avsnitt 3***Rättelse och radering***Artikel 16***Rätt till rättelse**

Den registrerade ska ha rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få felaktiga personuppgifter som rör honom eller henne rättade. Med beaktande av ändamålet med behandlingen, ska den registrerade ha rätt att komplettera ofullständiga personuppgifter, bland annat genom att tillhandahålla ett kompletterande utlåtande.

*Artikel 17***Rätt till radering ("rätten att bli bortglömd")**

1. Den registrerade ska ha rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få sina personuppgifter raderade och den personuppgiftsansvarige ska vara skyldig att utan onödigt dröjsmål radera personuppgifter om något av följande gäller:
 - a) Personuppgifterna är inte längre nödvändiga för de ändamål för vilka de samlats in eller på annat sätt behandlats.

- b) Den registrerade återkallar det samtycke på vilket behandlingen grundar sig enligt artikel 6.1 a eller artikel 9.2 a och det finns inte någon annan rättslig grund för behandlingen.
- c) Den registrerade invänder mot behandlingen i enlighet med artikel 21.1 och det saknas berättigade skäl för behandlingen som väger tyngre, eller den registrerade invänder mot behandlingen i enlighet med artikel 21.2.
- d) Personuppgifterna har behandlats på olagligt sätt.
- e) Personuppgifterna måste raderas för att uppfylla en rättslig förpliktelse i unionsrätten eller i medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av.
- f) Personuppgifterna har samlats in i samband med erbjudande av informationssamhällets tjänster, i de fall som avses i artikel 8.1.

2. Om den personuppgiftsansvarige har offentliggjort personuppgifterna och enligt punkt 1 är skyldig att radera personuppgifterna, ska den personuppgiftsansvarige med beaktande av tillgänglig teknik och kostnaden för genomförandet vidta rimliga åtgärder, inbegripet tekniska åtgärder, för att underrätta personuppgiftsansvariga som behandlar personuppgifterna om att den registrerade har begärt att de ska radera eventuella länkar till, eller kopior eller reproduktioner av dessa personuppgifter.

3. Punkterna 1 och 2 ska inte gälla i den utsträckning som behandlingen är nödvändig av följande skäl:

- a) För att utöva rätten till yttrande- och informationsfrihet.
- b) För att uppfylla en rättslig förpliktelse som kräver behandling enligt unionsrätten eller enligt en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av eller för att utföra en uppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den personuppgiftsansvarige.
- c) För skäl som rör ett viktigt allmänt intresse på folkhälsoområdet enligt artikel 9.2 h och i samt artikel 9.3.
- d) För arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål enligt artikel 89.1, i den utsträckning som den rätt som avses i punkt 1 sannolikt omöjliggör eller avsevärt försvårar uppnåendet av syftet med den behandlingen.
- e) För att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

Artikel 18

Rätt till begränsning av behandling

1. Den registrerade ska ha rätt att av den personuppgiftsansvarige kräva att behandlingen begränsas om något av följande alternativ är tillämpligt:

- a) Den registrerade bestrider personuppgifternas korrekthet, under en tid som ger den personuppgiftsansvarige möjlighet att kontrollera om personuppgifterna är korrekta.
- b) Behandlingen är olaglig och den registrerade motsätter sig att personuppgifterna raderas och i stället begär en begränsning av deras användning.
- c) Den personuppgiftsansvarige behöver inte längre personuppgifterna för ändamålen med behandlingen men den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.
- d) Den registrerade har invänt mot behandling i enlighet med artikel 21.1 i väntan på kontroll av huruvida den personuppgiftsansvariges berättigade skäl väger tyngre än den registrerades berättigade skäl.

2. Om behandlingen har begränsats i enlighet med punkt 1 får sådana personuppgifter, med undantag för lagring, endast behandlas med den registrerades samtycke eller för att fastställa, göra gällande eller försvara rättsliga anspråk eller för att skydda någon annan fysisk eller juridisk persons rättigheter eller för skäl som rör ett viktigt allmänintresse för unionen eller för en medlemsstat.

3. En registrerad som har fått behandling begränsad i enlighet med punkt 1 ska underrättas av den personuppgiftsansvarige innan begränsningen av behandlingen upphör.

Artikel 19

Anmälningsskyldighet avseende rättelse eller radering av personuppgifter och begränsning av behandling

Den personuppgiftsansvarige ska underrätta varje mottagare till vilken personuppgifterna har lämnats ut om eventuella rättelser eller radering av personuppgifter eller begränsningar av behandling som skett i enlighet med artiklarna 16, 17.1 och 18, om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Den personuppgiftsansvarige ska informera den registrerade om dessa mottagare på den registrerades begäran.

Artikel 20

Rätt till dataportabilitet

1. Den registrerade ska ha rätt att få ut de personuppgifter som rör honom eller henne och som han eller hon har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format och ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan att den personuppgiftsansvarige som tillhandahållits personuppgifterna hindrar detta, om

- a) behandlingen grundar sig på samtycke enligt artikel 6.1 a eller artikel 9.2 a eller på ett avtal enligt artikel 6.1 b, och
- b) behandlingen sker automatiserat.

2. Vid utövandet av sin rätt till dataportabilitet i enlighet med punkt 1 ska den registrerade ha rätt till överföring av personuppgifterna direkt från en personuppgiftsansvarig till en annan, när detta är tekniskt möjligt.

3. Utövandet av den rätt som avses i punkt 1 i den här artikeln ska inte påverka tillämpningen av artikel 17. Den rätten ska inte gälla i fråga om en behandling som är nödvändig för att utföra en uppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den personuppgiftsansvarige.

4. Den rätt som avses i punkt 1 får inte påverka andras rättigheter och friheter på ett ogynnsamt sätt.

Avsnitt 4

Rätt att göra invändningar och automatiserat individuellt beslutsfattande

Artikel 21

Rätt att göra invändningar

1. Den registrerade ska, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att när som helst göra invändningar mot behandling av personuppgifter avseende honom eller henne som grundar sig på artikel 6.1 e eller f, inbegripet profilering som grundar sig på dessa bestämmelser. Den personuppgiftsansvarige får inte längre behandla personuppgifterna såvida denne inte kan påvisa tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk.

2. Om personuppgifterna behandlas för direkt marknadsföring ska den registrerade ha rätt att när som helst invända mot behandling av personuppgifter som avser honom eller henne för sådan marknadsföring, vilket inkluderar profilering i den utsträckning som denna har ett samband med sådan direkt marknadsföring.

3. Om den registrerade invänder mot behandling för direkt marknadsföring ska personuppgifterna inte längre behandlas för sådana ändamål.

4. Senast vid den första kommunikationen med den registrerade ska den rätt som avses i punkterna 1 och 2 uttryckligen meddelas den registrerade och redovisas tydligt, klart och åtskilt från eventuell annan information.
5. När det gäller användningen av informationssamhällets tjänster, och trots vad som sägs i direktiv 2002/58/EG, får den registrerade utöva sin rätt att göra invändningar på automatiserat sätt med användning av tekniska specifikationer.
6. Om personuppgifter behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska den registrerade, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att göra invändningar mot behandling av personuppgifter avseende honom eller henne om inte behandlingen är nödvändig för att utföra en uppgift av allmänt intresse.

Artikel 22

Automatiserat individuellt beslutsfattande, inbegripet profilering

1. Den registrerade ska ha rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne.
2. Punkt 1 ska inte tillämpas om beslutet
 - a) är nödvändigt för ingående eller fullgörande av ett avtal mellan den registrerade och den personuppgiftsansvarige,
 - b) tillåts enligt unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av och som fastställer lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen, eller
 - c) grundar sig på den registrerades uttryckliga samtycke.
3. I fall som avses i punkt 2 a och c ska den personuppgiftsansvarige genomföra lämpliga åtgärder för att säkerställa den registrerades rättigheter, friheter och rättsliga intressen, åtminstone rätten till personlig kontakt med den personuppgiftsansvarige för att kunna uttrycka sin åsikt och bestrida beslutet.
4. Beslut enligt punkt 2 får inte grunda sig på de särskilda kategorier av personuppgifter som avses i artikel 9.1, såvida inte artikel 9.2 a eller g gäller och lämpliga åtgärder som ska skydda den registrerades berättigade intressen har vidtagits.

Avsnitt 5

Begränsningar

Artikel 23

Begränsningar

1. Det ska vara möjligt att i unionsrätten eller i en medlemsstats nationella rätt som den personuppgiftsansvarige eller personuppgiftsbiträdet omfattas av införa en lagstiftningsåtgärd som begränsar tillämpningsområdet för de skyldigheter och rättigheter som föreskrivs i artiklarna 12–22 och 34, samt artikel 5 i den mån dess bestämmelser motsvarar de rättigheter och skyldigheter som fastställs i artiklarna 12–22, om en sådan begränsning sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa
 - a) den nationella säkerheten,
 - b) försvaret,
 - c) den allmänna säkerheten,

- d) förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten,
 - e) andra av unionens eller en medlemsstats viktiga mål av generellt allmänt intresse, särskilt ett av unionens eller en medlemsstats viktiga ekonomiska eller finansiella intressen, däribland penning-, budget- eller skattefrågor, folkhälsa och social trygghet,
 - f) skydd av rättsväsendets oberoende och rättsliga åtgärder,
 - g) förebyggande, förhindrande, utredning, avslöjande och lagföring av överträdelser av etiska regler som gäller för lagreglerade yrken,
 - h) en tillsyns-, inspektions- eller regleringsfunktion som, även i enstaka fall, har samband med myndighetsutövning i fall som nämns i a–e och g,
 - i) skydd av den registrerade eller andras rättigheter och friheter,
 - j) verkställighet av civilrättsliga krav.
2. Framför allt ska alla lagstiftningsåtgärder som avses i punkt 1 innehålla specifika bestämmelser åtminstone, när så är relevant, avseende
- a) ändamålen med behandlingen eller kategorierna av behandling,
 - b) kategorierna av personuppgifter,
 - c) omfattningen av de införda begränsningarna,
 - d) skyddsåtgärder för att förhindra missbruk eller olaglig tillgång eller överföring,
 - e) specificeringen av den personuppgiftsansvarige eller kategorierna av personuppgiftsansvariga,
 - f) lagringstiden samt tillämpliga skyddsåtgärder med beaktande av behandlingens art, omfattning och ändamål eller kategorierna av behandling,
 - g) riskerna för de registrerades rättigheter och friheter, och
 - h) de registrerades rätt att bli informerade om begränsningen, såvida detta inte kan inverka menligt på begränsningen.

KAPITEL IV

Personuppgiftsansvarig och personuppgiftsbiträde

Avsnitt 1

Allmänna skyldigheter

Artikel 24

Den personuppgiftsansvariges ansvar

1. Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning. Dessa åtgärder ska ses över och uppdateras vid behov.
2. Om det står i proportion till behandlingen, ska de åtgärder som avses i punkt 1 omfatta den personuppgiftsansvariges genomförande av lämpliga strategier för dataskydd.
3. Tillämpningen av godkända uppförandekoder som avses i artikel 40 eller godkända certifieringsmekanismer som avses i artikel 42 får användas för att visa att den personuppgiftsansvarige fullgör sina skyldigheter.

*Artikel 25***Inbyggt dataskydd och dataskydd som standard**

1. Med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige, både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder – såsom pseudonymisering – vilka är utformade för ett effektivt genomförande av dataskyddsprinciper – såsom uppgiftsminimering – och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, så att kraven i denna förordning uppfylls och den registrerades rättigheter skyddas.
2. Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.
3. En godkänd certifieringsmekanism i enlighet med artikel 42 får användas för att visa att kraven i punkterna 1 och 2 i den här artikeln följs.

*Artikel 26***Gemensamt personuppgiftsansvariga**

1. Om två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga. Gemensamt personuppgiftsansvariga ska under öppna former fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt denna förordning, särskilt vad gäller utövandet av den registrerades rättigheter och sina respektive skyldigheter att tillhandahålla den information som avses i artiklarna 13 och 14, genom ett inbördes arrangemang, såvida inte de personuppgiftsansvarigas respektive skyldigheter fastställs genom unionsrätten eller en medlemsstats nationella rätt som de personuppgiftsansvariga omfattas av. Inom ramen för arrangemanget får en gemensam kontaktpunkt för de personuppgiftsansvariga utses.
2. Det arrangemang som avses i punkt 1 ska på lämpligt sätt återspegla de gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot registrerade. Det väsentliga innehållet i arrangemanget ska göras tillgängligt för den registrerade.
3. Oavsett formerna för det arrangemang som avses i punkt 1 får den registrerade utöva sina rättigheter enligt denna förordning med avseende på och emot var och en av de personuppgiftsansvariga.

*Artikel 27***Företrädare för personuppgiftsansvariga eller personuppgiftsbiträden som inte är etablerade i unionen**

1. Om artikel 3.2 tillämpas ska den personuppgiftsansvarige eller personuppgiftsbiträdet skriftligen utse en företrädare i unionen.
2. Skyldigheten enligt punkt 1 i denna artikel ska inte gälla
 - a) tillfällig behandling som inte omfattar behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1, eller behandling av personuppgifter avseende fällande domar i brottmål samt överträdelse, som avses i artikel 10, och som sannolikt inte kommer att medföra en risk för fysiska personers rättigheter och friheter, med hänsyn till behandlingens art, sammanhang, omfattning och ändamål, eller
 - b) en offentlig myndighet eller ett offentligt organ.

3. Företrädaren ska vara etablerad i en av de medlemsstater där de registrerade, vars personuppgifter behandlas i samband med att de erbjuds varor eller tjänster, eller vars beteende övervakas, befinner sig.
4. Företrädaren ska på den personuppgiftsansvariges eller personuppgiftsbitrådets uppdrag, utöver eller i stället för den personuppgiftsansvarige eller personuppgiftsbitrådet, fungera som kontaktperson för i synnerhet tillsynsmyndigheter och registrerade, i alla frågor som har anknytning till behandlingen, i syfte att säkerställa efterlevnad av denna förordning.
5. Att den personuppgiftsansvarige eller personuppgiftsbitrådet utser en företrädare ska inte påverka de rättsliga åtgärder som skulle kunna inledas mot den personuppgiftsansvarige eller personuppgiftsbitrådet.

Artikel 28

Personuppgiftsbiträden

1. Om en behandling ska genomföras på en personuppgiftsansvarigs vägnar ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning och säkerställer att den registrerades rättigheter skyddas.
2. Personuppgiftsbitrådet får inte anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgiftsansvarige. Om ett allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbitrådet informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden, så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar.
3. När uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbitrådet med avseende på den personuppgiftsansvarige och i vilken föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter anges. I det avtalet eller den rättsakten ska det särskilt föreskrivas att personuppgiftsbitrådet
 - a) endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, inbegripet när det gäller överföringar av personuppgifter till ett tredjeland eller en internationell organisation, såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbitrådet omfattas av, och i så fall ska personuppgiftsbitrådet informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt,
 - b) säkerställer att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt,
 - c) ska vidta alla åtgärder som krävs enligt artikel 32,
 - d) ska respektera de villkor som avses i punkterna 2 och 4 för anlitaandet av ett annat personuppgiftsbiträde,
 - e) med tanke på behandlingens art, ska hjälpa den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att den personuppgiftsansvarige kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter i enlighet med kapitel III,
 - f) ska bistå den personuppgiftsansvarige med att se till att skyldigheterna enligt artiklarna 32–36 fullgörs, med beaktande av typen av behandling och den information som personuppgiftsbitrådet har tillgång till,
 - g) beroende på vad den personuppgiftsansvarige väljer, ska radera eller återlämna alla personuppgifter till den personuppgiftsansvarige efter det att tillhandahållandet av behandlingstjänster har avslutats, och radera befintliga kopior såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt, och
 - h) ska ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som fastställs i denna artikel har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige.

Med avseende på led h i första stycket ska personuppgiftsbiträdet omedelbart informera den personuppgiftsansvarige om han anser att en instruktion strider mot denna förordning eller mot andra av unionens eller medlemsstaternas dataskyddsbestämmelser.

4. I de fall där ett personuppgiftsbiträde anlitar ett annat personuppgiftsbiträde för utförande av specifik behandling på den personuppgiftsansvariges vägnar ska det andra personuppgiftsbiträdet, genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt, åläggas samma skyldigheter i fråga om dataskydd som de som fastställs i avtalet eller den andra rättsakten mellan den personuppgiftsansvarige och personuppgiftsbiträdet enligt punkt 3, och framför allt att ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning. Om det andra personuppgiftsbiträdet inte fullgör sina skyldigheter i fråga om dataskydd ska det ursprungliga personuppgiftsbiträdet vara fullt ansvarig gentemot den personuppgiftsansvarige för utförandet av det andra personuppgiftsbiträdets skyldigheter.

5. Ett personuppgiftsbiträdes anslutning till en godkänd uppförandekod som avses i artikel 40 eller en godkänd certifieringsmekanism som avses i artikel 42 får användas för att visa att tillräckliga garantier tillhandahålls, så som avses punkterna 1 och 4 i den här artikeln.

6. Det avtal eller den andra rättsakt som avses i punkterna 3 och 4 i den här artikeln får, utan att det påverkar tillämpningen av ett enskilt avtal mellan den personuppgiftsansvarige och personuppgiftsbiträdet, helt eller delvis baseras på sådana standardavtalsklausuler som avses i punkterna 7 och 8 i den här artikeln, inbegripet när de ingår i en certifiering som i enlighet med artiklarna 42 och 43 beviljats den personuppgiftsansvarige eller personuppgiftsbiträdet.

7. Kommissionen får fastställa standardavtalsklausuler för de frågor som avses i punkterna 3 och 4 i den här artikeln, i enlighet med det granskningsförfarande som avses i artikel 93.2.

8. En tillsynsmyndighet får fastställa standardavtalsklausuler för de frågor som avses i punkterna 3 och 4 i den här artikeln, i enlighet med den mekanism för enhetlighet som avses i artikel 63.

9. Det avtal eller den andra rättsakt som avses i punkterna 3 och 4 ska upprättas skriftligen, inbegripet i ett elektroniskt format.

10. Om ett personuppgiftsbiträde överträder denna förordning genom att fastställa ändamålen med och medlen för behandlingen, ska personuppgiftsbiträdet anses vara personuppgiftsansvarig med avseende på den behandlingen, utan att det påverkar tillämpningen av artiklarna 82, 83 och 84.

Artikel 29

Behandling under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende

Personuppgiftsbiträdet och personer som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, får endast behandla dessa på instruktion från den personuppgiftsansvarige, såvida han eller hon inte är skyldig att göra det enligt unionsrätten eller medlemsstaternas nationella rätt.

Artikel 30

Register över behandling

1. Varje personuppgiftsansvarig och, i tillämpliga fall, dennes företrädare ska föra ett register över behandling som utförts under dess ansvar. Detta register ska innehålla samtliga följande uppgifter:

- a) Namn och kontaktuppgifter för den personuppgiftsansvarige, samt i tillämpliga fall gemensamt personuppgiftsansvarige, den personuppgiftsansvariges företrädare samt dataskyddsombudet.
- b) Ändamålen med behandlingen.
- c) En beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter.

- d) De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, inbegripet mottagare i tredjeländer eller i internationella organisationer.
- e) I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och, vid sådana överföringar som avses i artikel 49.1 andra stycket, dokumentationen av lämpliga skyddsåtgärder.
- f) Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.
- g) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1.
2. Varje personuppgiftsbiträde och, i tillämpliga fall, dennes företrädare ska föra ett register över alla kategorier av behandling som utförts för den personuppgiftsansvariges räkning, som omfattar följande:
- a) Namn och kontaktuppgifter för personuppgiftsbiträdet eller personuppgiftsbiträdena och för varje personuppgiftsansvarig för vars räkning personuppgiftsbiträdet agerar, och, i tillämpliga fall, för den personuppgiftsansvariges eller personuppgiftsbitrådets företrädare samt dataskyddsombudet.
- b) De kategorier av behandling som har utförts för varje personuppgiftsansvariges räkning.
- c) I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och, vid sådana överföringar som avses i artikel 49.1 andra stycket, dokumentationen av lämpliga skyddsåtgärder.
- d) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1.
3. De register som avses i punkterna 1 och 2 ska upprättas skriftligen, inbegripet i elektronisk form.
4. På begäran ska den personuppgiftsansvarige eller personuppgiftsbiträdet samt, i tillämpliga fall, den personuppgiftsansvariges eller personuppgiftsbitrådets företrädare göra registret tillgängligt för tillsynsmyndigheten.
5. De skyldigheter som anges i punkterna 1 och 2 ska inte gälla för ett företag eller en organisation som sysselsätter färre än 250 personer såvida inte den behandling som utförs sannolikt kommer att medföra en risk för registrerades rättigheter och friheter, behandlingen inte är tillfällig eller behandlingen omfattar särskilda kategorier av uppgifter som avses i artikel 9.1 eller personuppgifter om fällande domar i brottmål samt överträdelse som avses i artikel 10.

Artikel 31

Samarbete med tillsynsmyndigheten

Den personuppgiftsansvarige och personuppgiftsbiträdet samt, i tillämpliga fall, deras företrädare ska på begäran samarbeta med tillsynsmyndigheten vid utförandet av dennes uppgifter.

Avsnitt 2

Säkerhet för personuppgifter

Artikel 32

Säkerhet i samband med behandlingen

1. Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt

- a) pseudonymisering och kryptering av personuppgifter,

- b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,
 - c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,
 - d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.
2. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.
3. Anslutning till en godkänd uppförandekod som avses i artikel 40 eller en godkänd certifieringsmekanism som avses i artikel 42 får användas för att visa att kraven i punkt 1 i den här artikeln följs.
4. Den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvariges eller personuppgiftsbitrådets överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige, om inte unionsrätten eller medlemsstaternas nationella rätt ålägger honom eller henne att göra det.

Artikel 33

Anmälan av en personuppgiftsincident till tillsynsmyndigheten

1. Vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig i enlighet med artikel 55, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen.
2. Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident.
3. Den anmälan som avses i punkt 1 ska åtminstone
 - a) beskriva personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,
 - b) förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas,
 - c) beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och
 - d) beskriva de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.
4. Om och i den utsträckning det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.
5. Den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av denna artikel.

Artikel 34

Information till den registrerade om en personuppgiftsincident

1. Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten.

2. Den information till den registrerade som avses i punkt 1 i denna artikel ska innehålla en tydlig och klar beskrivning av personuppgiftsincidentens art och åtminstone de upplysningar och åtgärder som avses i artikel 33.3 b, c och d.
3. Information till den registrerade i enlighet med punkt 1 krävs inte om något av följande villkor är uppfyllt:
 - a) Den personuppgiftsansvarige har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder och dessa åtgärder tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten, i synnerhet sådana som ska göra uppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till personuppgifterna, såsom kryptering.
 - b) Den personuppgiftsansvarige har vidtagit ytterligare åtgärder som säkerställer att den höga risk för registrerades rättigheter och friheter som avses i punkt 1 sannolikt inte längre kommer att uppstå.
 - c) Det skulle inbegripa en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt.
4. Om den personuppgiftsansvarige inte redan har informerat den registrerade om personuppgiftsincidenten får tillsynsmyndigheten, efter att ha bedömt sannolikheten för att personuppgiftsincidenten medför en hög risk, kräva att personuppgiftsbiträdet gör det eller får besluta att något av de villkor som avses i punkt 3 uppfylls.

Avsnitt 3

Konsekvensbedömning avseende dataskydd samt föregående samråd

Artikel 35

Konsekvensbedömning avseende dataskydd

1. Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker.
2. Den personuppgiftsansvarige ska rådfråga dataskyddsombudet, om ett sådant utsetts, vid genomförande av en konsekvensbedömning avseende dataskydd.
3. En konsekvensbedömning avseende dataskydd som avses i punkt 1 ska särskilt krävas i följande fall:
 - a) En systematisk och omfattande bedömning av fysiska personers personliga aspekter som grundar sig på automatisk behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer.
 - b) Behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1, eller av personuppgifter som rör fällande domar i brottmål och överträdelse som avses i artikel 10.
 - c) Systematisk övervakning av en allmän plats i stor omfattning.
4. Tillsynsmyndigheten ska upprätta och offentliggöra en förteckning över det slags behandlingsverksamheter som omfattas av kravet på en konsekvensbedömning avseende dataskydd i enlighet med punkt 1. Tillsynsmyndigheten ska översända dessa förteckningar till den styrelse som avses i artikel 68.
5. Tillsynsmyndigheten får också upprätta och offentliggöra en förteckning över det slags behandlingsverksamheter som inte kräver någon konsekvensbedömning avseende dataskydd. Tillsynsmyndigheten ska översända dessa förteckningar till styrelsen.
6. Innan de förteckningar som avses i punkterna 4 och 5 antas ska den behöriga tillsynsmyndigheten tillämpa den mekanism för enhetlighet som avses i artikel 63 om en sådan förteckning inbegriper behandling som rör erbjudandet av varor eller tjänster till registrerade, eller övervakning av deras beteende i flera medlemsstater, eller som väsentligt kan påverka den fria rörligheten för personuppgifter i unionen.

7. Bedömningen ska innehålla åtminstone
 - a) en systematisk beskrivning av den planerade behandlingen och behandlingens syften, inbegripet, när det är lämpligt, den personuppgiftsansvariges berättigade intresse,
 - b) en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftena,
 - c) en bedömning av de risker för de registrerades rättigheter och friheter som avses i punkt 1, och
 - d) de åtgärder som planeras för att hantera riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna och för att visa att denna förordning efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.
8. De berörda personuppgiftsansvarigas eller personuppgiftsbiträdenas efterlevnad av godkända uppförandekoder enligt artikel 40 ska på lämpligt sätt beaktas vid bedömningen av konsekvenserna av de behandlingar som utförs av dessa personuppgiftsansvariga eller personuppgiftsbiträden, framför allt när det gäller att ta fram en konsekvensbedömning avseende dataskydd.
9. Den personuppgiftsansvarige ska, när det är lämpligt, inhämta synpunkter från de registrerade eller deras företrädare om den avsedda behandlingen, utan att det påverkar skyddet av kommersiella eller allmänna intressen eller behandlingens säkerhet.
10. Om behandling enligt artikel 6.1 c eller e har en rättslig grund i unionsrätten eller i en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av, reglerar den rätten den aktuella specifika behandlingsåtgärden eller serien av åtgärder i fråga och en konsekvensbedömning avseende dataskydd redan har genomförts som en del av en allmän konsekvensbedömning i samband med antagandet av denna rättsliga grund, ska punkterna 1–7 inte gälla, om inte medlemsstaterna anser det nödvändigt att utföra en sådan bedömning före behandlingen.
11. Den personuppgiftsansvarige ska vid behov genomföra en översyn för att bedöma om behandlingen genomförs i enlighet med konsekvensbedömningen avseende dataskydd åtminstone när den risk som behandlingen medför förändras.

Artikel 36

Förhandssamråd

1. Den personuppgiftsansvarige ska samråda med tillsynsmyndigheten före behandling om en konsekvensbedömning avseende dataskydd enligt artikel 35 visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken.
2. Om tillsynsmyndigheten anser att den planerade behandling som avses i punkt 1 skulle strida mot denna förordning, särskilt om den personuppgiftsansvarige inte i tillräcklig mån har fastställt eller reducerat risken, ska tillsynsmyndigheten inom en period på högst åtta veckor från det att begäran om samråd mottagits, ge den personuppgiftsansvarige och i tillämpliga fall personuppgiftsbiträdet skriftliga råd och får utnyttja alla de befogenheter som den har enligt artikel 58. Denna period får förlängas med sex veckor beroende på hur komplicerad den planerade behandlingen är. Tillsynsmyndigheten ska informera den personuppgiftsansvarige och, i tillämpliga fall, personuppgiftsbiträdet om en sådan förlängning inom en månad från det att begäran om samråd mottagits, tillsammans med orsakerna till förseningen. Dessa perioder får tillfälligt upphöra att löpa i avvaktan på att tillsynsmyndigheten erhåller den information som den har begärt med tanke på samrådet.
3. Vid samråd med tillsynsmyndigheten enligt punkt 1 ska den personuppgiftsansvarige till tillsynsmyndigheten lämna
 - a) i tillämpliga fall de respektive ansvarsområdena för de personuppgiftsansvariga, gemensamt personuppgiftsansvariga och personuppgiftsbiträden som medverkar vid behandlingen, framför allt vid behandling inom en koncern,
 - b) ändamålen med och medlen för den avsedda behandlingen,
 - c) de åtgärder som vidtas och de garantier som lämnas för att skydda de registrerades rättigheter och friheter enligt denna förordning,
 - d) i tillämpliga fall kontaktuppgifter till dataskyddsombudet,

- e) konsekvensbedömningen avseende dataskydd enligt artikel 35, och
- f) all annan information som begärs av tillsynsmyndigheten.

4. Medlemsstaterna ska samråda med tillsynsmyndigheten vid utarbetandet av ett förslag till lagstiftningsåtgärd som ska antas av ett nationellt parlament eller av en regleringsåtgärd som grundar sig på en sådan lagstiftningsåtgärd som rör behandling.

5. Trots vad som sägs i punkt 1 får det i medlemsstaternas nationella rätt krävas att personuppgiftsansvariga ska samråda med, och erhålla förhandstillstånd av, tillsynsmyndigheten när det gäller en personuppgiftsansvarigs behandling för utförandet av en uppgift som den personuppgiftsansvarige utför av allmänt intresse, inbegripet behandling avseende social trygghet och folkhälsa.

Avsnitt 4

Dataskyddsombud

Artikel 37

Utnämning av dataskyddsombudet

1. Den personuppgiftsansvarige och personuppgiftsbiträdet ska under alla omständigheter utnämna ett dataskyddsombud om
 - a) behandlingen genomförs av en myndighet eller ett offentligt organ, förutom när detta sker som en del av domstolarnas dömande verksamhet,
 - b) den personuppgiftsansvariges eller personuppgiftsbitrådets kärnverksamhet består av behandling som, på grund av sin karaktär, sin omfattning och/eller sina ändamål, kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning, eller
 - c) den personuppgiftsansvariges eller personuppgiftsbitrådets kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av uppgifter i enlighet med artikel 9 och personuppgifter som rör fällande domar i brottmål och överträdelse, som avses i artikel 10.
2. En koncern får utnämna ett enda dataskyddsombud om det på varje etableringsort är lätt att nå ett dataskyddsombud.
3. Om den personuppgiftsansvarige eller personuppgiftsbiträdet är en myndighet eller ett offentligt organ, får ett enda dataskyddsombud utnämnas för flera sådana myndigheter eller organ, med hänsyn till deras organisationsstruktur och storlek.
4. I andra fall än de som avses i punkt 1 får eller, om så krävs enligt unionsrätten eller medlemsstaternas nationella rätt, ska den personuppgiftsansvarige eller personuppgiftsbiträdet eller sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden utnämna ett dataskyddsombud. Dataskyddsombudet får agera för sådana sammanslutningar och andra organ som företräder personuppgiftsansvariga eller personuppgiftsbiträden.
5. Dataskyddsombudet ska utses på grundval av yrkesmässiga kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som avses i artikel 39.
6. Dataskyddsombudet får ingå i den personuppgiftsansvariges eller personuppgiftsbitrådets personal, eller utföra uppgifterna på grundval av ett tjänsteavtal.
7. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till tillsynsmyndigheten.

Artikel 38

Dataskyddsombudets ställning

1. Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.

2. Den personuppgiftsansvarige och personuppgiftsbiträdet ska stödja dataskyddsbudet i utförandet av de uppgifter som avses i artikel 39 genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter samt tillgång till personuppgifter och behandlingsförfaranden, samt i upprätthållandet av dennes sakkunskap.
3. Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att uppgiftskyddsbudet inte tar emot instruktioner som gäller utförandet av dessa uppgifter. Han eller hon får inte avsättas eller bli föremål för sanktioner av den personuppgiftsansvarige eller personuppgiftsbiträdet för att ha utfört sina uppgifter. Dataskyddsbudet ska rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbitrådets högsta förvaltningsnivå.
4. Den registrerade får kontakta dataskyddsbudet med avseende på alla frågor som rör behandlingen av dennes personuppgifter och utövandet av dennes rättigheter enligt denna förordning.
5. Dataskyddsbudet ska, när det gäller dennes genomförande av sina uppgifter, vara bundet av sekretess eller konfidentialitet i enlighet med unionsrätten eller medlemsstaternas nationella rätt.
6. Dataskyddsbudet får fullgöra andra uppgifter och uppdrag. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska se till att sådana uppgifter och uppdrag inte leder till en intressekonflikt.

Artikel 39

Dataskyddsbudets uppgifter

1. Dataskyddsbudet ska ha minst följande uppgifter:
 - a) Att informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar om deras skyldigheter enligt denna förordning och andra av unionens eller medlemsstaternas dataskyddsbestämmelser.
 - b) Att övervaka efterlevnaden av denna förordning, av andra av unionens eller medlemsstaternas dataskyddsbestämmelser och av den personuppgiftsansvariges eller personuppgiftsbitrådets strategi för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.
 - c) Att på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den enligt artikel 35.
 - d) Att samarbeta med tillsynsmyndigheten.
 - e) Att fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling, inbegripet det förhandssamråd som avses i artikel 36, och vid behov samråda i alla andra frågor.
2. Dataskyddsbudet ska vid utförandet av sina uppgifter ta vederbörlig hänsyn till de risker som är förknippade med behandling, med beaktande av behandlingens art, omfattning, sammanhang och syften.

Avsnitt 5

Uppförandekod och certifiering

Artikel 40

Uppförandekoder

1. Medlemsstaterna, tillsynsmyndigheterna, styrelsen och kommissionen ska uppmuntra utarbetandet av uppförandekoder avsedda att bidra till att denna förordning genomförs korrekt, med hänsyn till särdragen hos de olika sektorer där behandling sker, och de särskilda behoven hos mikroföretag samt små och medelstora företag.
2. Sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbitråden får utarbeta uppförandekoder, eller ändra eller utöka sådana koder, i syfte att specificera tillämpningen av denna förordning, till exempel när det gäller
 - a) rättvis och öppen behandling,

- b) personuppgiftsansvarigas berättigade intressen i särskilda sammanhang,
- c) insamling av personuppgifter,
- d) pseudonymisering av personuppgifter,
- e) information till allmänheten och de registrerade,
- f) utövande av registrerades rättigheter,
- g) information till och skydd av barn samt metoderna för att erhålla samtycke från de personer som har föräldransvar för barn,
- h) åtgärder och förfaranden som avses i artiklarna 24 och 25 samt åtgärder för att säkerställa säkerhet vid behandling i enlighet med artikel 32,
- i) anmälan av personuppgiftsincidenter till tillsynsmyndigheter och meddelande av sådana personuppgiftsincidenter till registrerade,
- j) överföring av personuppgifter till tredjeländer eller internationella organisationer,
- k) utomrättsliga förfaranden och andra tvistlösningsförfaranden för lösande av tvister mellan personuppgiftsansvariga och registrerade när det gäller behandling, utan att detta påverkar registrerades rättigheter enligt artiklarna 77 och 79.

3. Uppförandekoder som är godkända i enlighet med punkt 5 i denna artikel och som har allmän giltighet enligt punkt 9 i denna artikel får, förutom att de iakttas av personuppgiftsansvariga eller personuppgiftsbiträden som omfattas av denna förordning, även iakttas av personuppgiftsansvariga eller personuppgiftsbiträden som inte omfattas av denna förordning enligt artikel 3, för att tillhandahålla lämpliga garantier inom ramen för överföringar av personuppgifter till tredjeländer eller internationella organisationer enligt villkoren i artikel 46.2 e. Sådana personuppgiftsansvariga eller personuppgiftsbiträden ska göra bindande och verkställbara åtaganden, genom avtal eller andra rättsligt bindande instrument, att tillämpa dessa lämpliga garantier inbegripet när det gäller registrerades rättigheter.

4. Den uppförandekod som avses i punkt 2 i den här artikeln ska innehålla mekanismer som gör det möjligt för det organ som avses i artikel 41.1 att utföra den obligatoriska övervakningen av att dess bestämmelser efterlevs av personuppgiftsansvariga och personuppgiftsbiträden som tillämpar den, utan att det påverkar uppgifter eller befogenheter för de tillsynsmyndigheter som är behöriga enligt artikel 55 eller 56.

5. Sammanslutningar och andra organ som avses i punkt 2 i den här artikeln som avser att utarbeta en uppförandekod eller ändra eller utöka befintliga uppförandekoder ska inge utkastet till uppförandekod, ändringen eller utökningen till den tillsynsmyndighet som är behörig enligt artikel 55. Tillsynsmyndigheten ska yttra sig om huruvida utkastet till uppförandekod, ändring eller utökning överensstämmer med denna förordning och ska godkänna ett utkastet till kod, ändring eller utökning om den finner att tillräckliga garantier tillhandahålls.

6. Om utkastet till kod, eller en ändring eller utökning, godkänns i enlighet med punkt 5, och om den berörda uppförandekoden inte avser behandling i flera medlemsstater, ska tillsynsmyndigheten registrera och offentliggöra uppförandekoden.

7. Om ett utkast till uppförandekod avser behandling i flera medlemsstater ska den tillsynsmyndighet som är behörig enligt artikel 55 innan den godkänner utkastet till kod, ändring eller utökning, inom ramen för det förfarande som avses i artikel 63 överlämna det till styrelsen som ska avge ett yttrande om huruvida utkastet till kod, ändring eller utökning är förenligt med denna förordning eller, i de fall som avses i punkt 3 i den här artikeln, tillhandahåller lämpliga garantier.

8. Om det i det yttrande som avses i punkt 7 bekräftas att utkastet till kod, ändring eller utökning är förenligt med denna förordning, eller, i de fall som avses i punkt 3, tillhandahåller lämpliga garantier, ska styrelsen inlämna sitt yttrande till kommissionen.

9. Kommissionen får, genom genomförandeakter, besluta att den godkända koden, ändringen eller utökningen som getts in till den enligt punkt 8 i den här artikeln har allmän giltighet inom unionen. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

10. Kommissionen ska se till att de godkända koder om vilka det har beslutats att de har allmän giltighet enligt punkt 9 offentliggörs på lämpligt sätt.

11. Styrelsen ska samla alla godkända uppförandekoder, ändringar och utökningar i ett register och offentliggöra dem på lämpligt sätt.

Artikel 41

Övervakning av godkända uppförandekoder

1. Utan att det påverkar den berörda tillsynsmyndighetens uppgifter och befogenheter enligt artiklarna 57 och 58 får övervakningen av efterlevnaden av en uppförandekod i enlighet med artikel 40 utföras av ett organ som har en lämplig expertnivå i förhållande till kodens syfte och som ackrediteras för detta ändamål av den behöriga tillsynsmyndigheten.

2. Ett organ som avses i punkt 1 får ackrediteras för att övervaka efterlevnaden av en uppförandekod om detta organ har

a) visat sitt oberoende och sin expertis i förhållande till uppförandekodens syfte på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande,

b) upprättat förfaranden varigenom det kan bedöma de berörda personuppgiftsansvarigas och personuppgiftsbiträdenas lämplighet för att tillämpa uppförandekoden, övervaka att de efterlever dess bestämmelser och regelbundet se över hur den fungerar,

c) upprättat förfaranden och strukturer för att hantera klagomål om överträdelser av uppförandekoden eller det sätt på vilket uppförandekoden har tillämpats, eller tillämpas, av en personuppgiftsansvarig eller ett personuppgiftsbiträde, och för att göra dessa förfaranden och strukturer synliga för registrerade och för allmänheten, och

d) på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande visat att dess uppgifter och uppdrag inte leder till en intressekonflikt.

3. Den behöriga tillsynsmyndigheten ska inlämna utkastet till kriterier för ackreditering av ett organ som avses i punkt 1 i den här artikeln till styrelsen i enlighet med den mekanism för enhetlighet som avses i artikel 63.

4. Utan att det påverkar den behöriga tillsynsmyndighetens uppgifter och befogenheter och tillämpningen av bestämmelserna i kapitel VIII ska ett organ som avses i punkt 1 i denna artikel, med förbehåll för tillräckliga skyddsåtgärder, vidta lämpliga åtgärder i fall av en personuppgiftsansvarigs eller ett personuppgiftsbiträdes överträdelse av uppförandekoden, inbegripet avstängning eller uteslutande av den personuppgiftsansvarige eller personuppgiftsbiträdet från uppförandekoden. Det ska informera den behöriga tillsynsmyndigheten om sådana åtgärder och skälen för att de vidtagits.

5. Den behöriga tillsynsmyndigheten ska återkalla ackrediteringen av ett organ som avses i punkt 1 om villkoren för ackrediteringen inte, eller inte längre, uppfylls eller om åtgärder som vidtagits av organet strider mot denna förordning.

6. Denna artikel ska inte gälla behandling som utförs av offentliga myndigheter och organ.

Artikel 42

Certifiering

1. Medlemsstaterna, tillsynsmyndigheterna, styrelsen och kommissionen ska uppmuntra, särskilt på unionsnivå, införandet av certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd som syftar till att visa att personuppgiftsansvarigas eller personuppgiftsbiträdens behandling är förenlig med denna förordning. De särskilda behoven hos mikroföretag samt små och medelstora företag ska beaktas.

2. Certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd som är godkända enligt punkt 5 i denna artikel får, förutom att de iakttas av personuppgiftsansvariga eller personuppgiftsbiträden som omfattas av denna förordning, inrättas för att visa att det föreligger lämpliga garantier som tillhandahålls av personuppgiftsansvariga och personuppgiftsbiträden som inte omfattas av denna förordning enligt artikel 3, inom ramen för överföringar av personuppgifter till tredjeländer eller internationella organisationer enligt villkoren i artikel 46.2 f. Sådana personuppgiftsansvariga eller personuppgiftsbiträden ska göra bindande och verkställbara åtaganden, genom avtal eller andra rättsligt bindande instrument, att tillämpa dessa lämpliga garantier, inbegripet när det gäller registrerades rättigheter.
3. Certifieringen ska vara frivillig och tillgänglig via ett öppet förfarande.
4. En certifiering i enlighet med denna artikel minskar inte den personuppgiftsansvariges eller personuppgiftsbitrådets ansvar för att denna förordning efterlevs och påverkar inte uppgifter och befogenheter för de tillsynsmyndigheter som är behöriga enligt artikel 55 eller 56.
5. En certifiering i enlighet med denna artikel ska utfärdas av de certifieringsorgan som avses i artikel 43 eller av den behöriga tillsynsmyndigheten på grundval av kriterier som godkänts av den behöriga myndigheten enligt artikel 58.3 eller av styrelsen enligt artikel 63. Om kriterierna har godkänts av styrelsen får detta leda till en gemensam certifiering, det europeiska sigillet för dataskydd.
6. Den personuppgiftsansvarige eller det personuppgiftsbiträde som låter sin behandling av uppgifter omfattas av certifieringsmekanismen ska förse det certifieringsorgan som avses i artikel 43 eller, i tillämpliga fall, den behöriga tillsynsmyndigheten, med all information och tillgång till behandlingsförfaranden som krävs för att genomföra certifieringsförfarandet.
7. Certifiering ska utfärdas till en personuppgiftsansvarig eller ett personuppgiftsbiträde för en period på högst tre år och får förnyas på samma villkor under förutsättning att kraven fortsätter att vara uppfyllda. Certifiering ska, i tillämpliga fall, återkallas av de certifieringsorgan som avses i artikel 43 eller av den behöriga tillsynsmyndigheten om kraven för certifieringen inte eller inte längre uppfylls.
8. Styrelsen ska samla alla certifieringsmekanismer och sigill och märkningar för dataskydd i ett register och offentliggöra dem på lämpligt sätt.

Artikel 43

Certifieringsorgan

1. Utan att det påverkar den behöriga tillsynsmyndighetens uppgifter och befogenheter enligt artiklarna 57 och 58 ska certifieringsorgan som har lämplig nivå av expertis i fråga om dataskydd, efter att ha informerat tillsynsmyndigheten för att den ska kunna utöva sina befogenheter enligt artikel 58.2 h när så är nödvändigt, utfärda och förnya certifiering. Medlemsstat ska säkerställa att dessa certifieringsorgan är ackrediterade av en av eller båda följande:
 - a) Den tillsynsmyndighet som är behörig enligt artikel 55 eller 56,
 - b) det nationella ackrediteringsorgan som utsetts i enlighet med Europaparlamentets och rådets förordning (EG) nr 765/2008 ⁽¹⁾ i enlighet med EN-ISO/IEC 17065/2012 och med de ytterligare krav som fastställts av den tillsynsmyndighet som är behörig enligt artikel 55 eller 56.
2. Certifieringsorgan som avses i punkt 1 får ackrediteras i enlighet med den punkten endast om de har
 - a) visat oberoende och expertis i förhållande till certifieringens syfte på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande,

⁽¹⁾ Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknads kontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 (EUTL 218, 13.8.2008, s. 30).

- b) förbundet sig att respektera de kriterier som avses i artikel 42.5 och godkänts av den tillsynsmyndighet som är behörig enligt artikel 55 eller 56, eller av styrelsen enligt artikel 63,
- c) upprättat förfaranden för utfärdande, periodisk översyn och återkallande av certifiering, sigill och märkningar för dataskydd,
- d) upprättat förfaranden och strukturer för att hantera klagomål om överträdelser av certifieringen eller det sätt på vilket certifieringen har tillämpats, eller tillämpas, av en personuppgiftsansvarig eller ett personuppgiftsbiträde, och för att göra dessa förfaranden och strukturer synliga för registrerade och för allmänheten, och
- e) på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande visat att deras uppgifter och uppdrag inte leder till en intressekonflikt.

3. Ackrediteringen av certifieringsorgan som avses i punkterna 1 och 2 i denna artikel ska ske på grundval av kriterier som godkänts av den tillsynsmyndighet som är behörig enligt artikel 55 eller 56, eller av styrelsen enligt artikel 63. I händelse av ackreditering enligt punkt 1 b i den här artikeln ska dessa krav komplettera dem som föreskrivs i förordning (EG) nr 765/2008 och de tekniska regler som beskriver certifieringsorganens metoder och förfaranden.

4. De certifieringsorgan som avses i punkt 1 ska ansvara för den korrekta bedömning som leder till certifieringen eller återkallelsen av certifieringen, utan att det påverkar den personuppgiftsansvariges eller personuppgiftsbitrådets ansvar att efterleva denna förordning. Ackrediteringen ska utfärdas för en period på högst fem år och får förnyas på samma villkor under förutsättning att certifieringsorganet uppfyller de krav som anges i denna artikel.

5. De certifieringsorgan som avses i punkt 1 ska informera de behöriga tillsynsmyndigheterna om orsakerna till beviljandet eller återkallelsen av den begärda certifieringen.

6. De krav som avses i punkt 3 i den här artikeln och de kriterier som avses i artikel 42.5 ska offentliggöras av tillsynsmyndigheten i ett lättillgängligt format. Tillsynsmyndigheterna ska också översända dessa krav och kriterier till styrelsen. Styrelsen ska samla alla certifieringsmekanismer och sigill för dataskydd i ett register och offentliggöra dem på lämpligt sätt.

7. Utan att det påverkar tillämpningen av kapitel VIII ska den behöriga tillsynsmyndigheten eller det nationella ackrediteringsorganet återkalla ett certifieringsorgans ackreditering enligt punkt 1 i denna artikel om villkoren för ackrediteringen inte, eller inte längre, uppfylls eller om åtgärder som vidtagits av certifieringsorganet strider mot denna förordning.

8. Kommissionen ska ges befogenhet att anta delegerade akter i enlighet med artikel 92 i syfte att närmare ange de krav som ska tas i beaktande för de certifieringsmekanismer för dataskydd som avses i artikel 42.1.

9. Kommissionen får anta genomförandeakter för att fastställa tekniska standarder för certifieringsmekanismer och sigill och märkningar för dataskydd samt rutiner för att främja och erkänna dessa certifieringsmekanismer, sigill och märkningar. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

KAPITEL V

Överföring av personuppgifter till tredjeländer eller internationella organisationer

Artikel 44

Allmän princip för överföring av uppgifter

Överföring av personuppgifter som är under behandling eller är avsedda att behandlas efter det att de överförs till ett tredjeland eller en internationell organisation får bara ske under förutsättning att den personuppgiftsansvarige och personuppgiftsbiträdet, med förbehåll för övriga bestämmelser i denna förordning, uppfyller villkoren i detta kapitel, inklusive för vidare överföring av personuppgifter från tredjelandet eller den internationella organisationen till ett annat tredjeland eller en annan internationell organisation. Alla bestämmelser i detta kapitel ska tillämpas för att säkerställa att den nivå på skyddet av fysiska personer som säkerställs genom denna förordning inte undergrävs.

Artikel 45

Överföring på grundval av ett beslut om adekvat skyddsnivå

1. Personuppgifter får överföras till ett tredjeland eller en internationell organisation om kommissionen har beslutat att tredjelandet, ett territorium eller en eller flera specificerade sektorer i tredjelandet, eller den internationella organisationen i fråga säkerställer en adekvat skyddsnivå. En sådan överföring ska inte kräva något särskilt tillstånd.
 2. När kommissionen bedömer om en adekvat skyddsnivå föreligger ska den särskilt beakta
 - a) rättsstatsprincipen, respekten för de mänskliga rättigheterna och de grundläggande friheterna, relevant lagstiftning, både allmän lagstiftning och sektorslagstiftning, inklusive avseende allmän säkerhet, försvar, nationell säkerhet och straffrätt och offentliga myndigheters tillgång till personuppgifter samt tillämpningen av sådan lagstiftning, dataskyddsregler, yrkesregler och säkerhetsbestämmelser, inbegripet regler för vidare överföring av personuppgifter till ett annat tredjeland eller en annan internationell organisation, som ska följas i det landet eller den internationella organisationen, rättspraxis samt faktiska och verkställbara rättigheter för registrerade och effektiv administrativ och rättslig prövning för de registrerade vars personuppgifter överförs,
 - b) huruvida det finns en eller flera effektivt fungerande oberoende tillsynsmyndigheter i tredjelandet, eller som utövar tillsyn över den internationella organisationen, som har ansvar för att säkerställa och kontrollera att dataskyddsregler följs, inklusive lämpliga verkställighetsbefogenheter, ge de registrerade råd och assistans när det gäller utövandet av deras rättigheter och samarbeta med medlemsstaternas tillsynsmyndigheter, och
 - c) vilka internationella åtaganden det berörda tredjelandet eller den berörda internationella organisationen har gjort, eller andra skyldigheter som följer av rättsligt bindande konventioner eller instrument samt av dess deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter.
 3. Kommissionen får, efter att ha bedömt om det föreligger en adekvat skyddsnivå, genom en genomförandeakt besluta att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom ett tredjeland, eller en internationell organisation säkerställer en adekvat skyddsnivå i den mening som avses i punkt 2 i den här artikeln. Genomförandeakten ska inrätta en mekanism för regelbunden översyn, minst vart fjärde år, som ska beakta all relevant utveckling i det tredjelandet eller den internationella organisationen. Beslutets territoriella och sektorsmässiga tillämpning ska regleras i genomförandeakten, där det också i förekommande fall ska anges vilken eller vilka myndigheter som är tillsynsmyndighet(er) enligt punkt 2 b i den här artikeln. Genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.
 4. Kommissionen ska fortlöpande övervaka utveckling i tredjeländer och internationella organisationer vilken kan påverka hur beslut som antagits enligt punkt 3 i den här artikeln och beslut som antagits på grundval av artikel 25.6 i direktiv 95/46/EG fungerar.
 5. Kommissionen ska, när tillgänglig information visar, i synnerhet efter den översyn som avses i punkt 3 i den här artikeln, att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom tredjelandet i fråga eller en internationell organisation inte längre säkerställer adekvat skydd i den mening som avses i punkt 2 i den här artikeln och, i den mån det behövs, genom genomförandeakter återkalla, ändra eller upphäva det beslut som avses i punkt 3 i den här artikeln utan retroaktiv verkan. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.
- När det föreligger vederbörligen motiverade och tvingande skäl till skyndsamhet ska kommissionen anta omedelbart tillämpliga genomförandeakter i enlighet med det förfarande som avses i artikel 93.3.
6. Kommissionen ska samråda med tredjelandet eller den internationella organisationen i fråga för att lösa den situation som lett till beslutet enligt punkt 5.
 7. Beslut enligt punkt 5 i den här artikeln ska inte påverka överföring av personuppgifter till tredjelandet, ett territorium eller en eller flera specificerade sektorer inom tredjelandet, eller den internationella organisationen i fråga enligt artiklarna 46–49.
 8. Kommissionen ska i *Europeiska unionens officiella tidning* och på sin webbplats offentliggöra en förteckning över de tredjeländer och de territorier och specificerade sektorer i ett givet tredjeland samt de internationella organisationer för vilka den har fastställt att en adekvat skyddsnivå inte eller inte längre säkerställs.

9. De beslut som antas av kommissionen på grundval av artikel 25.6 i direktiv 95/46/EG ska förbli i kraft tills de ändrats, ersatts eller upphävts av ett kommissionsbeslut som antagits i enlighet med punkt 3 eller 5 i den här artikeln.

Artikel 46

Överföring som omfattas av lämpliga skyddsåtgärder

1. I avsaknad av ett beslut i enlighet med artikel 45.3, får en personuppgiftsansvarig eller ett personuppgiftsbiträde endast överföra personuppgifter till ett tredjeland eller en internationell organisation efter att ha vidtagit lämpliga skyddsåtgärder, och på villkor att lagstadgade rättigheter för registrerade och effektiva rättsmedel för registrerade finns tillgängliga.

2. Lämpliga skyddsåtgärder enligt punkt 1 får, utan att det krävs särskilt tillstånd från en övervakningsmyndighet, ta formen av

- a) ett rättsligt bindande och verkställbart instrument mellan offentliga myndigheter eller organ,
- b) bindande företagsbestämmelser i enlighet med artikel 47,
- c) standardiserade dataskyddsbestämmelser som antas av kommissionen i enlighet med det granskningsförfarande som avses i artikel 93.2,
- d) standardiserade dataskyddsbestämmelser som antagits av en tillsynsmyndighet och godkänts av kommissionen i enlighet med det granskningsförfarande som avses i artikel 93.2,
- e) en godkänd uppförandekod enligt artikel 40 tillsammans med rättsligt bindande och verkställbara åtaganden för den personuppgiftsansvarige eller personuppgiftsbiträdet i tredjelandet att tillämpa lämpliga skyddsåtgärder, även när det gäller registrerades rättigheter, eller
- f) en godkänd certifieringsmekanism enligt artikel 42 tillsammans med rättsligt bindande och verkställbara åtaganden för den personuppgiftsansvarige, personuppgiftsbiträdet i tredjelandet att tillämpa lämpliga skyddsåtgärder, även när det gäller de registrerades rättigheter.

3. Med förbehåll för tillstånd från den behöriga tillsynsmyndigheten, får lämpliga skyddsåtgärder enligt punkt 1 också i synnerhet ta formen av

- a) avtalsklausuler mellan den personuppgiftsansvarige eller personuppgiftsbiträdet och den personuppgiftsansvarige, personuppgiftsbiträdet eller mottagaren av personuppgifterna i tredjelandet eller den internationella organisationen, eller
- b) bestämmelser som ska införas i administrativa överenskommelser mellan offentliga myndigheter eller organ vilka inbegriper verkställbara och faktiska rättigheter för registrerade.

4. Tillsynsmyndigheten ska tillämpa den mekanism för enhetlighet som avses i artikel 63 i de fall som avses i punkt 3 i den här artikeln.

5. Tillstånd från en medlemsstat eller tillsynsmyndighet på grundval av artikel 26.2 i direktiv 95/46/EG ska förbli giltigt tills det, vid behov, ändrats, ersatts eller upphävts av den tillsynsmyndigheten. De beslut som fattas av kommissionen på grundval av artikel 26.4 i direktiv 95/46/EG ska förbli i kraft tills de, vid behov, ändrats, ersatts eller upphävts av ett kommissionsbeslut som antagits i enlighet med punkt 2 i den här artikeln.

Artikel 47

Bindande företagsbestämmelser

1. Den behöriga tillsynsmyndigheten ska godkänna bindande företagsbestämmelser i enlighet med den mekanism för enhetlighet som föreskrivs i artikel 63 under förutsättning att de

- a) är rättsligt bindande, tillämpas på, och verkställs av alla delar som berörs inom den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet, inklusive deras anställda,

- b) innehåller uttryckliga bestämmelser om de registrerades lagstadgade rättigheter när det gäller behandlingen av deras personuppgifter, och
 - c) uppfyller villkoren i punkt 2.
2. De bindande företagsbestämmelser som avses i punkt 1 ska närmare ange åtminstone följande:
- a) struktur och kontaktuppgifter för den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet och för var och en av dess medlemmar,
 - b) vilka överföringar eller uppsättningar av överföringar av uppgifter som omfattas, inklusive kategorierna av personuppgifter, typen av behandling och dess ändamål, den typ av registrerade som berörs samt vilket eller vilka tredjeländer som avses,
 - c) bestämmelsernas rättsligt bindande natur, såväl internt som externt,
 - d) tillämpningen av allmänna principer för dataskydd, särskilt avgränsning av syften, uppgiftsminimering, begränsade lagringsperioder, datakvalitet, inbyggt dataskydd och dataskydd som standard, rättslig grund för behandling, behandling av särskilda kategorier av personuppgifter, åtgärder för att säkerställa datasäkerhet och villkoren när det gäller vidare överföring av uppgifter till organ som inte är bundna av bindande företagsbestämmelser,
 - e) de registrerades rättigheter avseende behandling och medlen för att utöva dessa rättigheter, inklusive rätten att inte bli föremål för beslut grundade enbart på automatisk behandling, inklusive profilering, enligt artikel 22, rätten att inge klagomål till den behöriga tillsynsmyndigheten och till behöriga domstolar i medlemsstaterna enligt artikel 79, rätten till prövning samt i förekommande fall rätten till kompensation för överträdelse av de bindande företagsbestämmelserna,
 - f) att den personuppgiftsansvarige eller personuppgiftsbiträdet som är etablerad inom en medlemsstats territorium tar på sig ansvaret om en berörd enhet som inte är etablerad inom unionen bryter mot de bindande företagsbestämmelserna; den personuppgiftsansvarige eller personuppgiftsbiträdet får helt eller delvis undantas från denna skyldighet endast på villkor att det kan visas att den berörda enheten i företagsgruppen inte kan hållas ansvarig för den skada som har uppkommit,
 - g) hur de registrerade ska informeras om innehållet i de bindande företagsbestämmelserna, särskilt de bestämmelser som avses i leden d, e och f i denna punkt utöver den information som avses i artiklarna 13 och 14,
 - h) uppgifterna för varje dataskyddsombud som utsetts i enlighet med artikel 37, eller varje annan person eller enhet med ansvar för kontrollen av att de bindande företagsbestämmelserna följs inom den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet, samt i fråga om utbildning och hantering av klagomål,
 - i) förfaranden för klagomål,
 - j) rutinerna inom den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet för att kontrollera att de bindande företagsreglerna följs; sådana rutiner ska inbegripa dataskyddstillsyn och metoder för att säkerställa korrigerande åtgärder för att skydda de registrerades rättigheter; resultaten av sådana kontroller bör meddelas den person eller enhet som avses i led h och styrelsen i det kontrollerande företaget i koncernen eller gruppen av företag som deltar i gemensam ekonomisk verksamhet, och bör på begäran vara tillgänglig för den behöriga tillsynsmyndigheten,
 - k) rutinerna för att rapportera och dokumentera ändringar i bestämmelserna, samt rutinerna för att rapportera dessa ändringar till tillsynsmyndigheten,
 - l) rutinerna för att samarbeta med tillsynsmyndigheten i syfte att se till att alla medlemmar i den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet följer reglerna, särskilt genom att meddela tillsynsmyndigheten resultaten av kontroller av de åtgärder som avses i led j,
 - m) rutinerna för att till den behöriga tillsynsmyndigheten rapportera alla rättsliga krav som en medlem i koncernen eller gruppen av företag som deltar i gemensam ekonomisk verksamhet är underkastad i ett tredjeländ och som sannolikt kommer att ha en avsevärd negativ inverkan på de garantier som ges genom de bindande företagsbestämmelserna, och
 - n) lämplig utbildning om dataskydd för personal som har ständig eller regelbunden tillgång till personuppgifter.

3. Kommissionen får närmare ange vilket format och vilka rutiner som ska användas för de personuppgiftsansvarigas, personuppgiftsbiträdenas och tillsynsmyndigheternas utbyte av information om bindande företagsbestämmelser i den mening som avses i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

Artikel 48

Överföringar och utlämnanden som inte är tillåtna enligt unionsrätten

Domstolsbeslut eller beslut från myndigheter i tredjeland där det krävs att en personuppgiftsansvarig eller ett personuppgiftsbiträde överför eller lämnar ut personuppgifter får erkännas eller genomföras på något som helst sätt endast om det grundar sig på en internationell överenskommelse, såsom ett avtal om ömsesidig rättslig hjälp, som gäller mellan det begärande tredjelandet och unionen eller en medlemsstat, utan att detta påverkar andra grunder för överföring enligt detta kapitel.

Artikel 49

Undantag i särskilda situationer

1. Om det inte föreligger något beslut om adekvat skyddsnivå enligt artikel 45.3, eller om lämpliga skyddsåtgärder enligt artikel 46, inbegripet bindande företagsbestämmelser, får en överföring eller uppsättning av överföringar av personuppgifter till ett tredjeland eller en internationell organisation endast ske om något av följande villkor är uppfyllt:

- a) Den registrerade har uttryckligen samtyckt till att uppgifterna får överföras, efter att först ha blivit informerad om de eventuella riskerna med sådana överföringar för den registrerade när det inte föreligger något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder.
- b) Överföringen är nödvändig för att fullgöra ett avtal mellan den registrerade och den personuppgiftsansvarige eller för att genomföra åtgärder som föregår ett sådant avtal på den registrerades begäran.
- c) Överföringen är nödvändig för att ingå eller fullgöra ett avtal mellan den personuppgiftsansvarige och en annan fysisk eller juridisk person i den registrerades intresse.
- d) Överföringen är nödvändig av viktiga skäl som rör allmänintresset.
- e) Överföringen är nödvändig för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.
- f) Överföringen är nödvändig för att skydda den registrerades eller andra personers grundläggande intressen, när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.
- g) Överföringen görs från ett register som enligt unionsrätten eller medlemsstaternas nationella rätt är avsett att ge allmänheten information och som är tillgängligt antingen för allmänheten eller för var och en som kan styrka ett berättigat intresse, men endast i den utsträckning som de i unionsrätten eller i medlemsstaternas nationella rätt angivna villkoren för tillgänglighet uppfylls i det enskilda fallet.

När en överföring inte skulle kunna grundas på en bestämmelse i artikel 45 eller 46, inklusive bestämmelserna om bindande företagsbestämmelser, och inget av undantagen för en särskild situation som avses i första stycket i den här punkten är tillämpligt, får en överföring till ett tredjeland eller en internationell organisation äga rum endast om överföringen inte är repetitiv, endast gäller ett begränsat antal registrerade, är nödvändig för ändamål som rör den personuppgiftsansvariges tvingande berättigade intressen och den registrerades intressen eller rättigheter och friheter inte väger tyngre, och den personuppgiftsansvarige har bedömt samtliga omständigheter kring överföringen av uppgifter och på grundval av denna bedömning vidtagit lämpliga skyddsåtgärder för att skydda personuppgifter. Den personuppgiftsansvarige ska informera tillsynsmyndigheten om överföringen. Den personuppgiftsansvarige ska utöver tillhandahållande av den information som avses i artiklarna 13 och 14 informera den registrerade om överföringen och om de tvingande berättigade intressen som eftersträvas.

2. En överföring enligt led g i punkt 1 första stycket får inte omfatta alla personuppgifter eller hela kategorier av personuppgifter som finns i registret. Om registret är avsett att vara tillgängligt för personer med ett berättigat intresse ska överföringen göras endast på begäran av dessa personer eller om de själva är mottagarna.

3. Leden a, b och c i punkt 1 första stycket samt andra stycket i samma punkt ska inte gälla åtgärder som vidtas av offentliga myndigheter som ett led i myndighetsutövning.
4. Det allmänintresse som avses i led d i punkt 1 första stycket ska vara erkänt i unionsrätten eller i den nationella rätt som den personuppgiftsansvarige omfattas av.
5. Saknas beslut om adekvat skyddsnivå, får unionsrätten eller medlemsstaternas nationella rätt med hänsyn till viktiga allmänintressen uttryckligen fastställa gränser för överföringen av specifika kategorier av personuppgifter till ett tredjeländ eller en internationell organisation. Medlemsstaterna ska underrätta kommissionen om sådana bestämmelser.
6. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska bevara uppgifter både om bedömningen och om de lämpliga skyddsåtgärder som avses i punkt 1 andra stycket i den här artikeln i det register som avses i artikel 30.

Artikel 50

Internationellt samarbete för skydd av personuppgifter

När det gäller tredjeländer och internationella organisationer ska kommissionen och tillsynsmyndigheterna vidta lämpliga åtgärder för att

- a) utveckla rutiner för det internationella samarbetet för att underlätta en effektiv tillämpning av lagstiftningen om skydd av personuppgifter,
- b) på internationell nivå erbjuda ömsesidigt bistånd för en effektiv tillämpning av lagstiftningen om skydd av personuppgifter, bland annat genom underrättelse, hänskjutande av klagomål, bistånd vid utredningar samt informationsutbyte, med iakttagande av lämpliga skyddsåtgärder för personuppgifter samt skyddet av andra grundläggande rättigheter och friheter,
- c) involvera berörda aktörer i diskussioner och åtgärder som syftar till att öka det internationella samarbetet när det gäller tillämpningen av lagstiftningen om skydd av personuppgifter,
- d) främja utbyte och dokumentation om lagstiftning och praxis för skydd av personuppgifter, inklusive avseende behörighetskonflikter med tredjeländer.

KAPITEL VI

Oberoende tillsynsmyndigheter

Avsnitt 1

Oberoende ställning

Artikel 51

Tillsynsmyndighet

1. Varje medlemsstat ska föreskriva att en eller flera offentliga myndigheter ska vara ansvariga för att övervaka tillämpningen av denna förordning, i syfte att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling samt att underlätta det fria flödet av sådana uppgifter inom unionen (nedan kallad *tillsynsmyndighet*).
2. Varje tillsynsmyndighet ska bidra till en enhetlig tillämpning av denna förordning i hela unionen. För detta ändamål ska tillsynsmyndigheterna samarbeta såväl sinsemellan som med kommissionen i enlighet med kapitel VII.
3. Om det finns fler än en tillsynsmyndighet i en medlemsstat ska medlemsstaten utse den tillsynsmyndighet som ska företräda dessa myndigheter i styrelsen; medlemsstaten ska också upprätta en rutin för att se till att övriga myndigheter följer reglerna för den mekanism för enhetlighet som avses i artikel 63.
4. Varje medlemsstat ska senast den 25 maj 2018 anmäla till kommissionen vilka nationella bestämmelser den antar i enlighet med detta kapitel, och alla framtida ändringar som rör dessa bestämmelser ska anmälas utan dröjsmål.

*Artikel 52***Oberoende**

1. Varje tillsynsmyndighet ska vara fullständigt oberoende i utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med denna förordning.
2. Varje tillsynsmyndighets ledamot eller ledamöter ska i utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med denna förordning stå fria från utomstående påverkan, direkt såväl som indirekt, och får varken begära eller ta emot instruktioner av någon.
3. Tillsynsmyndighetens ledamöter ska avhålla sig från alla handlingar som är oförenliga med deras skyldigheter och under sin mandattid avstå från all annan avlönad eller oavlönad yrkesverksamhet som står i strid med deras tjänsteutövning.
4. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet förfogar över de personella, tekniska och finansiella resurser samt de lokaler och den infrastruktur som behövs för att myndigheten ska kunna utföra sina uppgifter och utöva sina befogenheter, inklusive inom ramen för det ömsesidiga biståndet, samarbetet och deltagandet i styrelsens verksamhet.
5. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet väljer och förfogar över egen personal, som ska ta instruktioner uteslutande från den berörda tillsynsmyndighetens ledamot eller ledamöter.
6. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet blir föremål för finansiell kontroll, utan att detta påverkar tillsynsmyndighetens oberoende och att de förfogar över en separat, offentlig årsbudget som kan ingå i den övergripande statsbudgeten eller nationella budgeten.

*Artikel 53***Allmänna villkor för tillsynsmyndighetens ledamöter**

1. Medlemsstaterna ska föreskriva att varje ledamot av deras tillsynsmyndigheter ska utnämnas genom ett genom ett öppet förfarande med insyn av
 - deras parlament,
 - deras regering,
 - deras statschef, eller
 - ett oberoende organ som genom medlemsstatens nationella rätt anförtrotts utnämningen.
2. Varje ledamot ska ha de kvalifikationer, den erfarenhet och den kompetens, särskilt på området skydd av personuppgifter, som krävs för att ledamoten ska kunna utföra sitt uppdrag och utöva sina befogenheter.
3. En ledamots uppdrag ska upphöra då mandattiden löper ut eller om ledamoten avgår eller avsätts från sin tjänst i enlighet med den berörda medlemsstatens nationella rätt.
4. En ledamot får avsättas endast på grund av grov försummelse eller när ledamoten inte längre uppfyller de villkor som krävs för att utföra uppdraget.

*Artikel 54***Regler för inrättandet av en tillsynsmyndighet**

1. Varje medlemsstat ska fastställa följande i lag:
 - a) Varje tillsynsmyndighets inrättande.

- b) De kvalifikationer och de villkor för lämplighet som krävs för att någon ska kunna utnännas till ledamot av en tillsynsmyndighet.
- c) Regler och förfaranden för att utse varje tillsynsmyndighets ledamot eller ledamöter.
- d) Mandattiden för varje tillsynsmyndighets ledamot eller ledamöter, vilken inte får understiga fyra år, utom vid tillsättandet av de första ledamöterna efter den 24 maj 2016, då ett stegvis tillsättningsförfarande med kortare perioder för några av ledamöterna får tillämpas om detta är nödvändigt för att säkerställa myndighetens oberoende.
- e) Huruvida varje tillsynsmyndighets ledamot eller ledamöter får ges förnyat mandat, och om så är fallet, för hur många perioder.
- f) Vilka villkor som gäller för de skyldigheter som varje tillsynsmyndighets ledamot eller ledamöter och personal har, förbud mot handlingar, yrkesverksamhet och förmåner som står i strid därmed under och efter mandattiden och vilka bestämmelser som gäller för anställningens upphörande.

2. Varje tillsynsmyndighets ledamot eller ledamöter och personal ska i enlighet med unionsrätten eller medlemsstaternas nationella rätt omfattas av tystnadsplikt både under och efter sin mandattid vad avser konfidentiell information som de fått kunskap om under utförandet av deras uppgifter eller utövandet av deras befogenheter. Under mandatperioden ska denna tystnadsplikt i synnerhet gälla rapportering från fysiska personer om överträdelse av denna förordning.

Avsnitt 2

Behörighet, uppgifter och befogenheter

Artikel 55

Behörighet

1. Varje tillsynsmyndighet ska vara behörig att utföra de uppgifter och utöva de befogenheter som tilldelas den enligt denna förordning inom sin egen medlemsstats territorium.
2. Om behandling utförs av myndigheter eller privata organ som agerar på grundval av artikel 6.1 c eller e ska tillsynsmyndigheten i den berörda medlemsstaten vara behörig. I sådana fall ska artikel 56 inte tillämpas.
3. Tillsynsmyndigheterna ska inte vara behöriga att utöva tillsyn över domstolar som behandlar personuppgifter i sin dömande verksamhet.

Artikel 56

Den ansvariga tillsynsmyndighetens behörighet

1. Utan att det påverkar tillämpningen av artikel 55 ska tillsynsmyndigheten för den personuppgiftsansvariges eller personuppgiftsbitrådets huvudsakliga verksamhetsställe eller enda verksamhetsställe vara behörig att agera som ansvarig tillsynsmyndighet för den personuppgiftsansvariges eller personuppgiftsbitrådets gränsöverskridande behandling i enlighet med det förfarande som föreskrivs i artikel 60.
2. Genom undantag från punkt 1 ska varje tillsynsmyndighet vara behörig att behandla ett klagomål som lämnats in till denna eller en eventuell överträdelse av denna förordning, om sakfrågan i ärendet endast rör ett verksamhetsställe i medlemsstaten eller i väsentlig grad påverkar registrerade endast i medlemsstaten.
3. I de fall som avses i punkt 2 i den här artikeln ska tillsynsmyndigheten utan dröjsmål informera den ansvariga tillsynsmyndigheten om detta ärende. Inom tre veckor från det att den underrättats ska den ansvariga tillsynsmyndigheten besluta huruvida den kommer att behandla ärendet i enlighet med det förfarande som föreskrivs i artikel 60, med hänsyn till huruvida den personuppgiftsansvarige eller personuppgiftsbitrådet har eller inte har ett verksamhetsställe som är beläget i den medlemsstat där den tillsynsmyndighet som lämnat informationen är belägen.

4. Om den ansvariga tillsynsmyndigheten beslutar att behandla ärendet ska det ske i enlighet med det förfarande som föreskrivs i artikel 60. Den tillsynsmyndighet som underrättade den ansvariga tillsynsmyndigheten får lämna in ett utkast till beslut till den ansvariga tillsynsmyndigheten. Den ansvariga tillsynsmyndigheten ska ta största möjliga hänsyn till detta utkast till beslut när det utarbetar det utkast till beslut som avses i artikel 60.3.
5. Om den ansvariga tillsynsmyndigheten beslutar att inte behandla ärendet ska den tillsynsmyndighet som underrättade den ansvariga tillsynsmyndigheten behandla ärendet i enlighet med artiklarna 61 och 62.
6. Den ansvariga tillsynsmyndigheten ska vara den personuppgiftsansvariges eller personuppgiftsbitrådets enda motpart när det gäller den registreringsansvariges eller den personuppgiftsbitrådets gränsöverskridande behandling.

Artikel 57

Uppgifter

1. Utan att det påverkar de andra uppgifter som föreskrivs i denna förordning ska varje tillsynsmyndighet på sitt territorium ansvara för följande:
 - a) Övervaka och verkställa tillämpningen av denna förordning.
 - b) Öka allmänhetens medvetenhet om och förståelse för risker, regler, skyddsåtgärder och rättigheter i fråga om behandling. Särskild uppmärksamhet ska ägnas åt insatser som riktar sig till barn.
 - c) I enlighet med medlemsstatens nationella rätt ge rådgivning åt det nationella parlamentet, regeringen och andra institutioner och organ om lagstiftningsåtgärder och administrativa åtgärder rörande skyddet av fysiska personers rättigheter och friheter när det gäller behandling.
 - d) Öka personuppgiftsansvarigas och personuppgiftsbitrådets medvetenhet om sina skyldigheter enligt denna förordning.
 - e) På begäran tillhandahålla information till registrerade om hur de ska utöva sina rättigheter enligt denna förordning, och om så krävs samarbeta med tillsynsmyndigheter i andra medlemsstater för detta ändamål.
 - f) Behandla klagomål från en registrerad eller från ett organ, en organisation eller en sammanslutning enligt artikel 80, och där så är lämpligt undersöka den sakfråga som klagomålet gäller och inom rimlig tid underrätta den enskilde om hur undersökningen fortskrider och om resultatet, i synnerhet om det krävs ytterligare undersökningar eller samordning med en annan tillsynsmyndighet.
 - g) Samarbeta, inbegripet utbyta information, med och ge ömsesidigt bistånd till andra tillsynsmyndigheter för att se till att denna förordning tillämpas och verkställs på ett enhetligt sätt.
 - h) Utföra undersökningar om tillämpningen av denna förordning, inbegripet på grundval av information som erhålls från en annan tillsynsmyndighet eller annan myndighet.
 - i) Följa sådan utveckling som påverkar skyddet av personuppgifter, bland annat inom informations- och kommunikationsteknik och affärspraxis.
 - j) Anta sådana standardavtalsklausuler som avses i artiklarna 28.8 och 46.2 d.
 - k) Upprätta och föra en förteckning när det gäller kravet på en konsekvensbedömning avseende dataskydd enligt artikel 35.4.
 - l) Ge råd om behandling av personuppgifter enligt artikel 36.2.
 - m) Främja framtagande av uppförandekoder enligt artikel 40.1 samt yttra sig över och godkänna sådana uppförandekoder som tillhandahåller tillräckliga garantier, i enlighet med artikel 40.5.
 - n) Uppmuntra till inrättandet av certifieringsmekanismer för dataskydd och av sigill och märkningar för dataskydd i enlighet med artikel 42.1 samt godkänna certifieringskriterierna i enlighet med artikel 42.5.
 - o) I tillämpliga fall genomföra en periodisk översyn av certifieringar som utfärdats i enlighet med artikel 42.7.

- p) Utarbeta och offentliggöra kriterier för ackreditering av ett organ för övervakning av uppförandekoder enligt artikel 41 och ett certifieringsorgan enligt artikel 43.
 - q) Ackreditera ett organ för övervakning av uppförandekoder enligt artikel 41 och ett certifieringsorgan enligt artikel 43.
 - r) Godkänna sådana avtalsklausuler och bestämmelser som avses i artikel 46.3.
 - s) Godkänna sådana bindande företagsbestämmelser som avses i artikel 47.
 - t) Bidra till styrelsens verksamhet.
 - u) Hålla arkiv över överträdelser av denna förordning och åtgärder som vidtagits i enlighet med artikel 58.2.
 - v) Utföra eventuella andra uppgifter som rör skyddet av personuppgifter.
2. Varje tillsynsmyndighet ska underlätta inlämningen av klagomål enligt punkt 1 f genom åtgärder såsom ett särskilt formulär för ändamålet, vilket också kan fyllas i elektroniskt, utan att andra kommunikationsformer utesluts.
3. Utförandet av alla tillsynsmyndigheters uppgifter ska vara avgiftsfritt för den registrerade och, i tillämpliga fall, för dataskyddsombudet.
4. Om en begäran är uppenbart ogrundad eller orimlig, särskilt på grund av dess repetitiva karaktär, får tillsynsmyndigheten ta ut en rimlig avgift grundad på de administrativa kostnaderna eller vägra att tillmötesgå begäran. Det åligger tillsynsmyndigheten att visa att begäran är uppenbart ogrundad eller orimlig.

Artikel 58

Befogenheter

1. Varje tillsynsmyndighet ska ha samtliga följande utredningsbefogenheter
- a) Beordra den personuppgiftsansvarige eller personuppgiftsbiträdet, och i tillämpliga fall den personuppgiftsansvariges eller personuppgiftsbitrådets företrädare, att lämna all information som myndigheten behöver för att kunna fullgöra sina uppgifter.
 - b) Genomföra undersökningar i form av dataskyddstillsyn.
 - c) Genomföra en översyn av certifieringar som utfärdats i enlighet med artikel 42.7.
 - d) Meddela den personuppgiftsansvarige eller personuppgiftsbiträdet om en påstådd överträdelse av denna förordning.
 - e) Från den personuppgiftsansvarige och personuppgiftsbiträdet få tillgång till alla personuppgifter och all information som tillsynsmyndigheten behöver för att kunna fullgöra sina uppgifter.
 - f) Få tillträde till alla lokaler som tillhör den personuppgiftsansvarige och personuppgiftsbiträdet, inbegripet tillgång till all utrustning och alla andra medel för behandling av personuppgifter i överensstämmelse med unionens processrätt eller medlemsstaternas nationella processrätt.
2. Varje tillsynsmyndighet ska ha samtliga följande korrigerande befogenheter
- a) Utfärda varningar till en personuppgiftsansvarig eller personuppgiftsbiträdet om att planerade behandlingar sannolikt kommer att bryta mot bestämmelserna i denna förordning.
 - b) Utfärda reprimander till en personuppgiftsansvarig eller personuppgiftsbiträdet om behandling bryter mot bestämmelserna i denna förordning.
 - c) Förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att tillmötesgå den registrerades begäran att få utöva sina rättigheter enligt denna förordning.

- d) Förelägga en personuppgiftsansvarig eller ett personuppgiftsbiträde att se till att behandlingen sker i enlighet med bestämmelserna i denna förordning och om så krävs på ett specifikt sätt och inom en specifik period,
- e) Förelägga den personuppgiftsansvarige att meddela den registrerade att en personuppgiftsincident har inträffat.
- f) Införa en tillfällig eller definitiv begränsning av, inklusive ett förbud mot, behandling.
- g) Förelägga om rättelse eller radering av personuppgifter samt begränsning av behandling enligt artiklarna 16, 17 och 18 och underrätta mottagare till vilka personuppgifterna har lämnats ut om dessa åtgärder enligt artiklarna 17.2 och 19.
- h) Återkalla en certifiering eller beordra certifieringsorganet att återkalla en certifiering som utfärdats enligt artikel 42 eller 43, eller beordra certifieringsorganet att inte utfärda certifiering om kraven för certifiering inte eller inte längre uppfylls.
- i) Påföra administrativa sanktionsavgifter i enlighet med artikel 83 utöver eller i stället för de åtgärder som avses i detta stycke, beroende på omständigheterna i varje enskilt fall.
- j) Förelägga om att flödet av uppgifter till en mottagare i tredje land eller en internationell organisation ska avbrytas.

3. Varje tillsynsmyndighet ska ha samtliga följande befogenheter att utfärda tillstånd och att ge råd:

- a) Ge råd till den personuppgiftsansvarige i enlighet med det förfarande för förhandssamråd som avses i artikel 36.
- b) På eget initiativ eller på begäran avge yttranden till det nationella parlamentet, medlemsstatens regering eller, i enlighet med medlemsstatens nationella rätt, till andra institutioner och organ samt till allmänheten, i frågor som rör skydd av personuppgifter.
- c) Ge tillstånd till behandling enligt artikel 36.5 om medlemsstatens rätt kräver ett sådant förhandstillstånd.
- d) Avge ett yttrande om och godkänna utkast till uppförandekoder enligt artikel 40.5.
- e) Ackreditera certifieringsorgan i enlighet med artikel 43.
- f) Utfärda certifieringar och godkänna kriterier för certifiering i enlighet med artikel 42.5.
- g) Anta standardiserade dataskyddsbestämmelser enligt artiklarna 28.8 och 46.2 d.
- h) Godkänna avtalsklausuler enligt artikel 46.3 a.
- i) Godkänna administrativa överenskommelser enligt artikel 46.3 b.
- j) Godkänna bindande företagsbestämmelser enligt artikel 47.

4. Utövandet av de befogenheter som tillsynsmyndigheten tilldelas enligt denna artikel ska omfattas av lämpliga skyddsåtgärder, inbegripet effektiva rättsmedel och rättssäkerhet, som fastställs i unionsrätten och i medlemsstaternas nationella rätt i enlighet med stadgan.

5. Varje medlemsstat ska i lagstiftning fastställa att dess tillsynsmyndighet ska ha befogenhet att upplysa de rättsliga myndigheterna om överträdelse av denna förordning och vid behov att inleda eller på övrigt vis delta i rättsliga förfaranden, för att verkställa bestämmelserna i denna förordning.

6. Varje medlemsstat får i lagstiftning föreskriva att dess tillsynsmyndighet ska ha ytterligare befogenheter utöver dem som avses i punkterna 1, 2 och 3. Utövandet av dessa befogenheter ska inte påverka den effektiva tillämpningen av kapitel VII.

Artikel 59

Verksamhetsrapporter

Varje tillsynsmyndighet ska upprätta en årlig rapport om sin verksamhet, vilken kan omfatta en förteckning över typer av anmälda överträdelse och typer av åtgärder som vidtagits i enlighet med artikel 58.2. Rapporterna ska översändas till det nationella parlamentet, regeringen och andra myndigheter som utsetts genom medlemsstatens nationella rätt. De ska göras tillgängliga för allmänheten, kommissionen och styrelsen.

KAPITEL VII

Samarbete och enhetlighet

Avsnitt 1

Samarbete

Artikel 60

Samarbete mellan den ansvariga tillsynsmyndigheten och de andra berörda tillsynsmyndigheterna

1. Den ansvariga tillsynsmyndigheten ska samarbeta med de andra berörda tillsynsmyndigheterna i enlighet med denna artikel i en strävan att uppnå samförstånd. Den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna ska utbyta all relevant information med varandra.
2. Den ansvariga tillsynsmyndigheten får när som helst begära att andra berörda tillsynsmyndigheter ger ömsesidigt bistånd i enlighet med artikel 61 och får genomföra gemensamma insatser i enlighet med artikel 62, i synnerhet för att utföra utredningar eller övervaka genomförandet av en åtgärd som avser en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad i en annan medlemsstat.
3. Den ansvariga tillsynsmyndigheten ska utan dröjsmål meddela de andra berörda tillsynsmyndigheterna den relevanta informationen i ärendet. Den ska utan dröjsmål lägga fram ett utkast till beslut för de andra berörda tillsynsmyndigheterna så att de kan avge ett yttrande och ta vederbörlig hänsyn till deras synpunkter.
4. Om någon av de andra berörda tillsynsmyndigheterna inom en period av fyra veckor efter att de har rådfrågats i enlighet med punkt 3 i den här artikeln uttrycker en relevant och motiverad invändning mot utkastet till beslut ska den ansvariga tillsynsmyndigheten, om den inte instämmer i den relevanta och motiverade invändningen eller anser att invändningen inte är relevant eller motiverad, överlämna ärendet till den mekanism för enhetlighet som avses i artikel 63.
5. Om den ansvariga tillsynsmyndigheten avser att följa den relevanta och motiverade invändningen ska den till de andra berörda tillsynsmyndigheterna överlämna ett reviderat utkast till beslut så att de kan avge ett yttrande. Detta reviderade utkast till beslut ska omfattas av det förfarande som avses i punkt 4 inom en period av två veckor.
6. Om ingen av de andra berörda tillsynsmyndigheterna har gjort invändningar mot det utkast till beslut som den ansvariga tillsynsmyndigheten har lagt fram inom den period som avses i punkterna 4 och 5 ska den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna anses samtycka till detta utkast till beslut och ska vara bundna av det.
7. Den ansvariga tillsynsmyndigheten ska anta och meddela beslutet till den personuppgiftsansvariges eller personuppgiftsbitrådets huvudsakliga eller enda verksamhetsställe, allt efter omständigheterna, och underrätta de andra berörda tillsynsmyndigheterna och styrelsen om beslutet i fråga, inbegripet en sammanfattning av relevanta fakta och en relevant motivering. Den tillsynsmyndighet till vilken ett klagomål har lämnats in ska underrätta den enskilde om beslutet.
8. Om ett klagomål avvisas eller avslås ska den tillsynsmyndighet till vilken klagomålet lämnades in, genom undantag från punkt 7, anta beslutet och meddela den enskilde samt informera den personuppgiftsansvarige.
9. Om den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna är överens om att avvisa eller avslå delar av ett klagomål och att vidta åtgärder beträffande andra delar av klagomålet ska ett separat beslut antas för var och en av dessa delar av frågan. Den ansvariga tillsynsmyndigheten ska anta beslutet om den del som gäller åtgärder som avser den personuppgiftsansvarige och meddela det till den personuppgiftsansvariges eller personuppgiftsbitrådets huvudsakliga eller enda verksamhetsställe på medlemsstatens territorium och underrätta den enskilde om detta, medan den enskildes tillsynsmyndighet ska anta beslutet för den del som gäller avvisande av eller avslag på klagomålet och meddela det till den enskilde och underrätta den personuppgiftsansvarige eller personuppgiftsbiträdet om detta.
10. Efter att den personuppgiftsansvarige eller personuppgiftsbiträdet har meddelats om den ansvariga myndighetens beslut i enlighet med punkterna 7 och 9 ska den personuppgiftsansvarige eller personuppgiftsbiträdet vidta nödvändiga åtgärder för att se till att beslutet efterlevs vad gäller behandling med koppling till alla deras verksamhetsställen i unionen. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska meddela den ansvariga tillsynsmyndigheten vilka åtgärder som har vidtagits för att efterleva beslutet, och den ansvariga tillsynsmyndigheten ska informera de andra berörda tillsynsmyndigheterna.

11. Om en berörd tillsynsmyndighet under exceptionella omständigheter har skäl att anse att det finns ett brådskande behov av att agera för att skydda registrerades intressen ska det skyndsamma förfarande som avses i artikel 66 tillämpas.
12. Den ansvariga tillsynsmyndigheten och de andra berörda tillsynsmyndigheterna ska förse varandra med den information som krävs enligt denna artikel på elektronisk väg med användning av ett standardiserat format.

Artikel 61

Ömsesidigt bistånd

1. Tillsynsmyndigheterna ska utbyta relevant information och ge ömsesidigt bistånd i arbetet för att genomföra och tillämpa denna förordning på ett enhetligt sätt, och ska införa åtgärder som bidrar till ett verkningsfullt samarbete. Det ömsesidiga biståndet ska i synnerhet omfatta begäranden om information och tillsynsåtgärder, till exempel begäranden om utförande av förhandstillstånd och förhandssamråd, inspektioner och utredningar.
2. Varje tillsynsmyndighet ska vidta lämpliga åtgärder som krävs för att besvara en begäran från en annan tillsynsmyndighet utan onödigt dröjsmål och inte senare än en månad efter det att den tagit emot begäran. Till sådana åtgärder hör bland annat att översända relevant information om genomförandet av en pågående utredning.
3. En begäran om bistånd ska innehålla all nödvändig information, inklusive syftet med begäran och skälen till denna. Information som utbyts får endast användas för det syfte för vilket den har begärts.
4. Den tillsynsmyndighet som tar emot en begäran får endast vägra att tillmötesgå begäran om
 - a) den inte är behörig att behandla den sakfråga som begäran avser eller de åtgärder som det begärs att den ska utföra, eller
 - b) det skulle stå i strid med denna förordning eller unionsrätten eller den nationella rätt i en medlemsstat som tillsynsmyndigheten omfattas av att tillmötesgå begäran.
5. Den tillsynsmyndighet som tagit emot begäran ska meddela den myndighet som begäran kommer ifrån om resultatet eller, allt efter omständigheterna, om hur de åtgärder som vidtagits för att tillmötesgå begäran fortskrider. Den tillsynsmyndighet som tagit emot begäran ska redogöra för sina skäl för att vägra tillmötesgå begäran i enlighet med punkt 4.
6. Den tillsynsmyndighet som tar emot en begäran ska som regel tillhandahålla den information som begärts av andra tillsynsmyndigheter på elektronisk väg med användning av ett standardiserat format.
7. Tillsynsmyndigheter som tar emot en begäran får inte ta ut någon avgift för åtgärder som vidtagits av dem till följd av en begäran om ömsesidigt bistånd. Tillsynsmyndigheter får i undantagsfall komma överens med andra tillsynsmyndigheter om regler för ersättning från varandra för vissa utgifter i samband med tillhandahållande av ömsesidigt bistånd.
8. Om en tillsynsmyndighet inte tillhandahåller den information som avses i punkt 5 i denna artikel inom en månad efter det att den erhållit begäran från en annan tillsynsmyndighet får den begärande myndigheten anta en provisorisk åtgärd på sin medlemsstats territorium i enlighet med artikel 55.1. I detta fall ska det brådskande behov av att agera enligt artikel 66.1 anses vara uppfyllt och kräva ett brådskande bindande beslut från styrelsen i enlighet med artikel 66.2.
9. Kommissionen får genom genomförandeakter närmare ange format och förfaranden för sådant ömsesidigt bistånd som avses i denna artikel samt formerna för elektronisk överföring av information tillsynsmyndigheter emellan, samt mellan tillsynsmyndigheter och styrelsen, i synnerhet det standardiserade format som avses i punkt 6 i den här artikeln. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

Artikel 62

Tillsynsmyndigheters gemensamma insatser

1. Tillsynsmyndigheter ska vid behov genomföra gemensamma insatser, inbegripet gemensamma utredningar och gemensamma verkställighetsåtgärder i vilka ledamöter eller personal från andra medlemsstaters tillsynsmyndigheter deltar.

2. Om den personuppgiftsansvarige eller personuppgiftsbiträdet har verksamhetsställen i flera medlemsstater eller om ett betydande antal registrerade personer i mer än en medlemsstat sannolikt kommer att påverkas i väsentlig grad av att uppgifter behandlas, ska tillsynsmyndigheterna i var och en av dessa medlemsstater ha rätt att delta i de gemensamma insatserna. Den tillsynsmyndighet som är behörig enligt artikel 56.1 eller 56.4 ska bjuda in tillsynsmyndigheterna i var och en av de berörda medlemsstaterna att delta i de gemensamma insatserna och ska utan dröjsmål svara på en annan tillsynsmyndighets begäran att få delta.
3. En tillsynsmyndighet får, i enlighet med medlemsstatens nationella rätt och efter godkännande från ursprungslandets tillsynsmyndighet, tilldela befogenheter, inklusive utredningsbefogenheter, till ledamöter eller personal från ursprungslandets tillsynsmyndighet som deltar i gemensamma insatser eller, i den mån lagstiftningen i den medlemsstat som är värdland för tillsynsmyndigheten tillåter detta, medge att ursprungslandets tillsynsmyndighets ledamöter eller personal utövar utredningsbefogenheter enligt lagstiftningen i ursprungslandets tillsynsmyndighets medlemsstat. Sådana utredningsbefogenheter får endast utövas under vägledning och i närvaro av ledamöter eller personal från värdlandets tillsynsmyndighet. Ledamöter och personal från ursprungslandets tillsynsmyndighet ska omfattas av den medlemsstats nationella rätt som gäller för värdlandets tillsynsmyndighet.
4. Om personal från ursprungslandets tillsynsmyndighet verkar i en annan medlemsstat i enlighet med punkt 1 ska värdtillsynsmyndighetens medlemsstat ansvara för deras handlingar, vilket inbegriper ansvar för skador som personalen vållar i samband med insatserna, i enlighet med rätten i den medlemsstat på vars territorium personalen verkar.
5. Den medlemsstat på vars territorium skadorna förorsakades ska ersätta sådana skador enligt de villkor som gäller för skador som förorsakas av dess egen personal. Den medlemsstat vars tillsynsmyndighets tjänstemän har orsakat en person skada på någon annan medlemsstats territorium ska fullt ut ersätta den andra medlemsstaten för det belopp som denna har betalat ut till den personens rättsinnehavare.
6. Utan att det påverkar rättigheterna gentemot tredje man och tillämpningen av punkt 5, ska varje medlemsstat i de fall som nämns i punkt 1 avstå från att kräva ersättning från en annan medlemsstat för skador som avses i punkt 4.
7. Om en gemensam insats planeras och en tillsynsmyndighet inte inom en månad har uppfyllt sin skyldighet enligt punkt 2 i den här artikeln, andra meningens övriga tillsynsmyndigheter anta provisoriska åtgärder på sina respektive medlemsstaters territorium i enlighet med artikel 55. I detta fall ska det brådskande behov av att agera enligt artikel 66.1 anses vara uppfyllt och kräva ett yttrande eller ett brådskande bindande beslut från styrelsen i enlighet med artikel 66.2.

Avsnitt 2

Enhetlighet

Artikel 63

Mekanism för enhetlighet

För att bidra till en enhetlig tillämpning av denna förordning i hela unionen ska tillsynsmyndigheterna samarbeta med varandra och, i förekommande fall, med kommissionen, genom den mekanism för enhetlighet som föreskrivs i detta avsnitt.

Artikel 64

Yttrande från Styrelsen

1. Styrelsen ska avge ett yttrande när en behörig tillsynsmyndighet avser att anta någon av åtgärderna nedan. I detta syfte ska den behöriga tillsynsmyndigheten skicka utkastet till beslut till styrelsen när det
 - a) syftar till att anta en förteckning över behandling som omfattas av kravet på en konsekvensbedömning avseende dataskydd enligt artikel 35.4,
 - b) rör ett ärende i enlighet med artikel 40.7 om huruvida ett utkast till uppförandekoder eller en ändring eller förlängning av en uppförandekod är förenlig med denna förordning,

- c) syftar till att godkänna kriterierna för ackreditering av ett organ enligt artikel 41.3 eller ett certifieringsorgan enligt artikel 43.3,
- d) syftar till att fastställa standardiserade dataskyddsbestämmelser enligt artiklarna 46.2 d och 28.8,
- e) syftar till att godkänna sådana avtalsklausuler som avses i artikel 46.3 a, eller
- f) syftar till att godkänna bindande företagsbestämmelser enligt artikel 47.

2. Varje tillsynsmyndighet, styrelsens ordförande eller kommissionen får i syfte att erhålla ett yttrande begära att styrelsen granskar en fråga med allmän räckvidd eller som har följder i mer än en medlemsstat, i synnerhet om en behörig myndighet inte uppfyller sina skyldigheter i fråga om ömsesidigt bistånd i enlighet med artikel 61 eller i fråga om gemensamma insatser i enlighet med artikel 62.

3. I de fall som avses i punkterna 1 och 2 ska styrelsen avge ett yttrande i den fråga som ingivits till den, förutsatt att den inte redan har avgett ett yttrande i samma fråga. Detta yttrande ska antas med enkel majoritet av styrelsens ledamöter inom åtta veckor. Denna period får förlängas med ytterligare sex veckor med hänsyn till sakfrågans komplexitet. Vad gäller det utkast till beslut som avses i punkt 1 som spridits till styrelsens ledamöter i enlighet med punkt 5, ska en ledamot som inte har gjort invändningar inom en rimlig period som ordföranden angett anses samtycka till utkastet till beslut.

4. Tillsynsmyndigheterna och kommissionen ska utan onödigt dröjsmål i ett standardiserat elektroniskt format till styrelsen översända all relevant information, som allt efter omständigheterna får utgöras av en sammanfattning av sakförhållanden, utkastet till beslut, grunden till att en sådan åtgärd är nödvändig och synpunkter från övriga berörda tillsynsmyndigheter.

5. Styrelsens ordförande ska utan onödigt dröjsmål och på elektronisk väg upplysa

- a) styrelsens ledamöter samt kommissionen om all relevant information som meddelats styrelsen i ett standardiserat format; styrelsens sekretariat ska vid behov tillhandahålla översättningar av relevant information; och
- b) den tillsynsmyndighet som, allt efter omständigheterna, avses i punkterna 1 och 2 samt kommissionen om yttrandet, och ska också offentliggöra det.

6. Den behöriga tillsynsmyndigheten får inte anta sitt utkast till beslut enligt punkt 1 inom den period som avses i punkt 3.

7. Den tillsynsmyndighet som avses i punkt 1 ska ta största möjliga hänsyn till styrelsens yttrande och ska, inom två veckor efter att yttrandet inkommit, i ett standardiserat elektroniskt format meddela styrelsens ordförande om huruvida den kommer att hålla fast vid eller ändra sitt utkast till beslut, och i förekommande fall översända det ändrade utkastet till beslut.

8. Om den berörda tillsynsmyndigheten underrättar styrelsens ordförande inom den period som avses i punkt 7 i den här artikeln om att den inte avser att följa styrelsens yttrande, helt eller delvis, och tillhandahåller en relevant motivering, ska artikel 65.1 tillämpas.

Artikel 65

Twistlösning genom styrelsen

1. För att säkerställa en korrekt och enhetlig tillämpning av denna förordning i enskilda fall ska styrelsen anta ett bindande beslut i följande fall:

- a) Om en berörd tillsynsmyndighet i ett fall som avses i artikel 60.4 har gjort en relevant och motiverad invändning mot ett utkast till beslut av den ansvariga myndigheten, eller om den ansvariga myndigheten har avslagit denna invändning med motiveringen att den inte var relevant eller motiverad. Det bindande beslutet ska avse alla ärenden som är föremål för den relevanta och motiverade invändningen, särskilt frågan om huruvida det föreligger en överträdelse av denna förordning.

- b) Om det finns motstridiga åsikter om vilken av de berörda tillsynsmyndigheterna som är behörig för det huvudsakliga verksamhetsstället.
- c) Om en behörig tillsynsmyndighet inte begär ett yttrande från styrelsen i de fall som avses i artikel 64.1, eller inte följer ett yttrande som styrelsen avger enligt artikel 64. I detta fall får varje berörd tillsynsmyndighet eller kommissionen översända ärendet till styrelsen.
2. Det beslut som avses i punkt 1 ska antas inom en månad efter det att sakfrågan hänskjutits med två tredjedels majoritet av styrelsens ledamöter. Denna period får förlängas med ytterligare en månad med hänsyn till sakfrågans komplexitet. Det beslut som avses i punkt 1 ska vara motiverat och riktat till den ansvariga tillsynsmyndigheten och alla berörda tillsynsmyndigheter och ska vara bindande för dem.
3. Om styrelsen inte har kunnat anta något beslut inom de perioder som avses i punkt 2 ska den anta sitt beslut inom två veckor efter utgången av den andra månad som avses i punkt 2 med enkel majoritet av styrelsens ledamöter. Om styrelsens ledamöter är delade i frågan ska beslutet antas i enlighet med ordförandens röst.
4. De berörda tillsynsmyndigheterna ska inte anta något beslut om den sakfråga som ingivits till styrelsen i enlighet med punkt 1 under de perioder som avses i punkterna 2 och 3.
5. Styrelsens ordförande ska utan onödigt dröjsmål meddela de berörda tillsynsmyndigheterna det beslut som avses i punkt 1. Kommissionen ska informeras om detta. Beslutet ska utan dröjsmål offentliggöras på styrelsens webbplats efter att tillsynsmyndigheten har meddelat det slutliga beslut som avses i punkt 6.
6. Den ansvariga tillsynsmyndigheten eller, allt efter omständigheterna, den tillsynsmyndighet till vilken klagomålet har ingetts ska anta sitt slutliga beslut på grundval av det beslut som avses i punkt 1 i den här artikeln, utan onödigt dröjsmål och senast en månad efter det att styrelsen har meddelat sitt beslut. Den ansvariga tillsynsmyndigheten eller, allt efter omständigheterna, den tillsynsmyndighet till vilken klagomålet har ingetts ska underrätta styrelsen om vilken dag dess slutliga beslut meddelas till den personuppgiftsansvarige respektive personuppgiftsbiträdet och den registrerade. De berörda tillsynsmyndigheternas slutliga beslut ska antas i enlighet med bestämmelserna i artikel 60.7, 60.8 och 60.9. Det slutliga beslutet ska hänvisa till det beslut som avses i punkt 1 i den här artikeln och ska precisera att det beslut som avses i punkt 1 kommer att offentliggöras på styrelsens webbplats i enlighet med punkt 5 i den här artikeln. Det beslut som avses i punkt 1 i den här artikeln ska fogas till det slutliga beslutet.

Artikel 66

Skyndsamt förfarande

1. Under exceptionella omständigheter får en berörd tillsynsmyndighet med avvikelse från den mekanism för enhetlighet som avses i artiklarna 63, 64 och 65 eller det förfarande som avses i artikel 60 omedelbart vidta provisoriska åtgärder avsedda att ha rättsverkan på det egna territoriet och med förutbestämd varaktighet som inte överskrider tre månader, om den anser att det finns ett brådskande behov av att agera för att skydda registrerades rättigheter och friheter. Tillsynsmyndigheten ska utan dröjsmål underrätta de andra berörda tillsynsmyndigheterna, styrelsen och kommissionen om dessa åtgärder och om skälen till att de vidtas.
2. Om en tillsynsmyndighet har vidtagit en åtgärd enligt punkt 1 och anser att definitiva åtgärder skyndsamt måste antas, får den begära ett brådskande yttrande eller ett brådskande bindande beslut från styrelsen; den ska då motivera varför den begär ett sådant yttrande eller beslut.
3. Om en behörig tillsynsmyndighet inte har vidtagit någon lämplig åtgärd i en situation som kräver skyndsamt handling för att skydda registrerades rättigheter och friheter, får vilken tillsynsmyndighet som helst begära ett brådskande yttrande eller, i tillämpliga fall, ett brådskande bindande beslut från styrelsen, varvid den ska motivera varför den begär ett sådant yttrande eller beslut och varför åtgärden måste vidtas skyndsamt.
4. Genom undantag från artiklarna 64.3 och 65.2 ska ett brådskande yttrande eller ett brådskande beslut enligt punkterna 2 och 3 i den här artikeln antas inom två veckor med enkel majoritet av styrelsens ledamöter.

*Artikel 67***Utbyte av information**

Kommissionen får anta genomförandeakter med allmän räckvidd i syfte att närmare ange tillvägagångssätten för elektroniskt utbyte av information mellan tillsynsmyndigheter samt mellan tillsynsmyndigheter och styrelsen, särskilt det standardiserade format som avses i artikel 64.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

*Avsnitt 3***Europeiska dataskyddsstyrelsen***Artikel 68***Europeiska dataskyddsstyrelsen**

1. Europeiska dataskyddsstyrelsen (nedan kallad *styrelsen*) inrättas härmed som ett unionsorgan och ska ha ställning som juridisk person.
2. Styrelsen ska företrädas av sin ordförande.
3. Styrelsen ska bestå av chefen för en tillsynsmyndighet per medlemsstat och av Europeiska datatillsynsmannen eller deras respektive företrädare.
4. Om en medlemsstat har mer än en tillsynsmyndighet som ansvarar för att övervaka tillämpningen av bestämmelserna i denna förordning ska en gemensam företrädare utses i enlighet med den medlemsstatens nationella rätt.
5. Kommissionen ska ha rätt att delta i styrelsens verksamhet och möten utan rösträtt. Kommissionen ska utse en egen företrädare. Styrelsens ordförande ska underrätta kommissionen om styrelsens verksamhet.
6. I de fall som avses i artikel 65 ska Europeiska datatillsynsmannen endast ha rösträtt i fråga om beslut som rör principer och regler som är tillämpliga på unionens institutioner, organ och byråer, och som i allt väsentligt motsvarar dem i denna förordning.

*Artikel 69***Oberoende**

1. Styrelsen ska vara oberoende när den fullgör sina uppgifter eller utövar sina befogenheter i enlighet med artiklarna 70 och 71.
2. Utan att detta påverkar kommissionens rätt att lämna en begäran enligt artikel 70.1 b och 70.2 ska styrelsen när den fullgör sina uppgifter eller utövar sina befogenheter varken begära eller ta emot instruktioner av någon.

*Artikel 70***Styrelsens uppgifter**

1. Styrelsen ska se till att denna förordning tillämpas enhetligt. För detta ändamål ska styrelsen, på eget initiativ eller i förekommande fall på begäran av kommissionen, i synnerhet
 - a) övervaka och säkerställa korrekt tillämpning av denna förordning i de fall som avses i artiklarna 64 och 65 utan att det påverkar de nationella tillsynsmyndigheternas uppgifter,

- b) ge kommissionen råd i alla frågor som gäller skydd av personuppgifter inom unionen, inklusive om eventuella förslag till ändring av denna förordning,
- c) ge kommissionen råd om format och förfaranden för informationsutbyte mellan personuppgiftsansvariga, personuppgiftsbiträden och tillsynsmyndigheter för bindande företagsbestämmelser,
- d) utfärda riktlinjer, rekommendationer och bästa praxis beträffande förfaranden för att radera länkar, kopior eller reproduktioner av personuppgifter från allmänt tillgängliga kommunikationstjänster enligt artikel 17.2,
- e) på eget initiativ eller på begäran av en av sina ledamöter eller av kommissionen behandla frågor om tillämpningen av denna förordning och utfärda riktlinjer, rekommendationer och bästa praxis i syfte att främja en enhetlig tillämpning av denna förordning,
- f) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att närmare ange kriterierna och villkoren för profileringsbaserade beslut enligt artikel 22.2,
- g) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att konstatera sådana personuppgiftsincidenter och fastställa sådant onödigt dröjsmål som avses i artikel 33.1 och 33.2 och för de särskilda omständigheter under vilka en personuppgiftsansvarig eller ett personuppgiftsbiträde är skyldig att anmäla personuppgiftsincidenten,
- h) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt angående de omständigheter under vilka en personuppgiftsincident sannolikt kommer att leda till hög risk för rättigheterna och friheterna för de fysiska personer som avses i artikel 34.1,
- i) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att närmare ange kriterierna och kraven för överföringar av personuppgifter på grundval av bindande företagsbestämmelser som personuppgiftsansvariga eller personuppgiftsbiträden följer samt ytterligare nödvändiga krav för att säkerställa skyddet för personuppgifter för berörda registrerade enligt artikel 47,
- j) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att närmare ange kriterierna och villkoren för överföring av personuppgifter på grundval av artikel 49.1,
- k) utforma riktlinjer för tillsynsmyndigheterna i fråga om tillämpningen av de åtgärder som avses i artikel 58.1, 58.2 och 58.3 och fastställandet av administrativa sanktionsavgifter i enlighet med artikel 83,
- l) se över den praktiska tillämpningen av de riktlinjer och rekommendationer samt den bästa praxis som avses i leden e och f,
- m) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att fastställa gemensamma förfaranden för fysiska personers rapportering av överträdelser av denna förordning enligt artikel 54.2,
- n) främja utarbetandet av uppförandekoder och införandet av certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd i enlighet med artiklarna 40 och 42,
- o) ackreditera certifieringsorgan och utföra sin periodiska översyn i enlighet med artikel 43 och föra ett offentligt register över ackrediterade organ i enlighet med artikel 43.6 och över de ackrediterade personuppgiftsansvariga eller personuppgiftsbiträdena som är etablerade i tredjeländer i enlighet med artikel 42.7,
- p) närmare ange de krav som avses i artikel 43.3 i syfte att ackreditera certifieringsorgan enligt artikel 42,
- q) avge ett yttrande till kommissionen om de certifieringskrav som avses i artikel 43.8,
- r) avge ett yttrande till kommissionen om de symboler som avses i artikel 12.7,
- s) avge ett yttrande till kommissionen för bedömningen av adekvat skyddsnivå i ett tredjeland eller en internationell organisation, inklusive för bedömningen av huruvida ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom det tredjelandet, eller en internationell organisation inte längre säkerställer en adekvat skyddsnivå; i detta syfte ska kommissionen lämna all nödvändig dokumentation till styrelsen, inklusive korrespondens med regeringen i tredjelandet, med avseende på tredjelandet, territoriet eller den specificerade sektorn, eller till databehandlingssektorn i tredjelandet eller den internationella organisationen,

- t) avge yttranden om utkast till beslut som läggs fram av tillsynsmyndigheter inom den mekanism för enhetlighet som avses i artikel 64.1, i ärenden som ingivits i enlighet med artikel 64.2 och anta bindande beslut i enlighet med artikel 65, inbegripet de fall som avses i artikel 66,
 - u) främja samarbete och effektivt bilateralt och multilateralt utbyte av bästa praxis och information mellan tillsynsmyndigheterna,
 - v) främja gemensamma utbildningsprogram och underlätta personalutbyte mellan tillsynsmyndigheterna och där så är lämpligt även med tillsynsmyndigheter i tredjeländer eller internationella organisationer,
 - w) främja utbyte av kunskap och dokumentation om lagstiftning om och praxis för dataskydd med tillsynsmyndigheter för dataskydd i hela världen.
 - x) avge yttranden över de uppförandekoder som utarbetas på unionsnivå i enlighet med artikel 40.9, och
 - y) föra ett offentligt elektroniskt register över tillsynsmyndigheters beslut och domstolars avgöranden i frågor som hanteras inom mekanismen för enhetlighet.
2. När kommissionen begär rådgivning från styrelsen får den ange en tidsfrist med hänsyn till hur brådskande ärendet är.
 3. Styrelsen ska vidarebefordra sina yttranden, riktlinjer, rekommendationer och bästa praxis till kommissionen och till den kommitté som avses i artikel 93, samt offentliggöra dem.
 4. När så är lämpligt ska styrelsen samråda med berörda parter och ge dem möjlighet att yttra sig inom rimlig tid. Styrelsen ska, utan att det påverkar tillämpningen av artikel 76, offentliggöra resultatet av samrådsförfarandet.

Artikel 71

Rapporter

1. Styrelsen ska sammanställa en årsrapport om skydd av fysiska personer vid behandling inom unionen och, i förekommande fall, i tredjeländer och internationella organisationer. Rapporten ska offentliggöras och översändas till Europaparlamentet, rådet och kommissionen.
2. Årsrapporten ska också innehålla en översikt över den praktiska tillämpningen av de riktlinjer och rekommendationer och den bästa praxis som avses i artikel 70.1 liksom de bindande beslut som avses i artikel 65.

Artikel 72

Förfarande

1. Styrelsen ska fatta beslut med enkel majoritet av dess ledamöter, om inte annat anges i denna förordning.
2. Styrelsen ska själv anta sin arbetsordning med två tredjedels majoritet av sina ledamöter och fastställa sina arbetsformer.

Artikel 73

Ordförande

1. Styrelsen ska med enkel majoritet välja en ordförande och två vice ordförande bland sina ledamöter.
2. Ordförandens och de vice ordförandenas mandattid ska vara fem år och kunna förnyas en gång.

*Artikel 74***Ordförandens uppgifter**

1. Ordföranden ska ha i uppgift att
 - a) sammankalla till styrelsens möten och planera dagordningen,
 - b) meddela beslut som antas av styrelsen i enlighet med artikel 65 till den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna,
 - c) se till att styrelsens uppgifter fullgörs i tid, särskilt i fråga om den mekanism för enhetlighet som avses i artikel 63.
2. Fördelningen av uppgifter mellan ordföranden och de vice ordförandena ska fastställas i styrelsens arbetsordning.

*Artikel 75***Sekretariatet**

1. Styrelsen ska förfoga över ett sekretariat som ska tillhandahållas av Europeiska datatillsynsmannen.
2. Sekretariatet ska utföra sina uppgifter enbart under ledning av ordföranden för styrelsen.
3. Den personal vid Europeiska datatillsynsmannen som utför de uppgifter som styrelsen tilldelas genom denna förordning ska följa separata rapporteringsvägar från den personal som utför de uppgifter som Europeiska datatillsynsmannen tilldelas.
4. När så är lämpligt ska styrelsen och Europeiska datatillsynsmannen fastställa och offentliggöra ett samförståndsavtal för genomförande av denna artikel, som fastställer villkoren för deras samarbete, och som ska tillämpas på den personal vid Europeiska datatillsynsmannen som utför de uppgifter som styrelsen tilldelas genom denna förordning.
5. Sekretariatet ska förse styrelsen med analysstöd samt administrativt och logistiskt stöd.
6. Sekretariatet ska särskilt ansvara för
 - a) styrelsens löpande arbete,
 - b) kommunikationen mellan styrelsens ledamöter, dess ordförande och kommissionen,
 - c) kommunikationen med andra institutioner och med allmänheten,
 - d) användningen av elektroniska medel för intern och extern kommunikation,
 - e) översättning av relevant information,
 - f) förberedelser och uppföljning av styrelsens möten,
 - g) förberedelse, sammanställning och offentliggörande av yttranden, beslut om lösning av tvister mellan tillsynsmyndigheter och andra texter som antas av styrelsen.

*Artikel 76***Konfidentialitet**

1. Styrelsens överläggningar ska vara konfidentiella i de fall som styrelsen bedömer detta vara nödvändigt, i enlighet med vad som anges i dess arbetsordning.

2. Tillgången till handlingar som skickas till styrelsens ledamöter, till experter eller till företrädare för tredje part ska regleras av Europaparlamentets och rådets förordning (EG) nr 1049/2001 ⁽¹⁾.

KAPITEL VIII

Rättsmedel, ansvar och sanktioner

Artikel 77

Rätt att lämna in klagomål till en tillsynsmyndighet

1. Utan att det påverkar något annat administrativt prövningsförfarande eller rättsmedel, ska varje registrerad som anser att behandlingen av personuppgifter som avser henne eller honom strider mot denna förordning ha rätt att lämna in ett klagomål till en tillsynsmyndighet, särskilt i den medlemsstat där han eller hon har sin hemvist eller sin arbetsplats eller där det påstådda intrånget begicks.

2. Den tillsynsmyndighet till vilken klagomålet har ingetts ska underrätta den enskilde om hur arbetet med klagomålet fortskrider och vad resultatet blir, inbegripet möjligheten till rättslig prövning enligt artikel 78.

Artikel 78

Rätt till ett effektivt rättsmedel mot tillsynsmyndighetens beslut

1. Utan att det påverkar något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol ska varje fysisk eller juridisk person ha rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut rörande dem som meddelats av en tillsynsmyndighet.

2. Utan att det påverkar något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol, ska varje registrerad person ha rätt till ett effektivt rättsmedel om den tillsynsmyndighet som är behörig i enlighet med artiklarna 55 och 56 underlåter att behandla ett klagomål eller att informera den registrerade inom tre månader om hur det fortskrider med det klagomål som ingetts med stöd av artikel 77 eller vilket beslut som har fattats med anledning av det.

3. Talan mot en tillsynsmyndighet ska väckas vid domstolarna i den medlemsstat där tillsynsmyndigheten har sitt säte.

4. Om talan väcks mot ett beslut som fattats av en tillsynsmyndighet och som föregicks av ett yttrande från eller beslut av styrelsen inom ramen för mekanismen för enhetlighet ska tillsynsmyndigheten vidarebefordra detta yttrande eller beslut till domstolen.

Artikel 79

Rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde

1. Utan att det påverkar tillgängliga administrativa prövningsförfaranden eller prövningsförfaranden utanför domstol, inbegripet rätten att lämna in ett klagomål till en tillsynsmyndighet i enlighet med artikel 77, ska varje registrerad som anser att hans eller hennes rättigheter enligt denna förordning har åsidosatts som en följd av att hans eller hennes personuppgifter har behandlats på ett sätt som inte är förenligt med denna förordning ha rätt till ett effektivt rättsmedel.

2. Talan mot en personuppgiftsansvarig eller ett personuppgiftsbiträde ska väckas vid domstolarna i den medlemsstat där den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad. Alternativt får sådan talan väckas vid domstolarna i den medlemsstat där den registrerade har sin hemvist, såvida inte den personuppgiftsansvarige eller personuppgiftsbiträdet är en myndighet i en medlemsstat som agerar inom ramen för sin myndighetsutövning.

⁽¹⁾ Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar (EGT L 145, 31.5.2001, s. 43).

*Artikel 80***Företrädande av registrerade**

1. Den registrerade ska ha rätt att ge ett organ, en organisation eller sammanslutning utan vinstsyfte, som har inrättats på lämpligt sätt i enlighet med lagen i en medlemsstat, vars stadgeenliga mål är av allmänt intresse och som är verksam inom området skydd av registrerades rättigheter och friheter när det gäller skyddet av deras personuppgifter, i uppdrag att lämna in ett klagomål för hans eller hennes räkning, att utöva de rättigheter som avses i artiklarna 77, 78 och 79 för hans eller hennes räkning samt att för hans eller hennes räkning utöva den rätt till ersättning som avses i artikel 82 om så föreskrivs i medlemsstatens nationella rätt.
2. Medlemsstaterna får föreskriva att ett organ, en organisation eller en sammanslutning enligt punkt 1 i den här artikeln, oberoende av en registrerads mandat, har rätt att i den medlemsstaten inge klagomål till den tillsynsmyndighet som är behörig enligt artikel 77 och utöva de rättigheter som avses i artiklarna 78 och 79 om organet, organisationen eller sammanslutningen anser att den registrerades rättigheter enligt den här förordningen har kränkts som en följd av behandlingen.

*Artikel 81***Vilandeförklaring av förfaranden**

1. Om en behörig domstol i en medlemsstat har information om att förfaranden som rör samma sakfråga vad gäller behandling av samma personuppgiftsansvarige eller personuppgiftsbiträde pågår i en domstol i en annan medlemsstat ska den kontakta denna domstol i den andra medlemsstaten för att bekräfta förekomsten av sådana förfaranden.
2. Om förfaranden som rör samma sakfråga vad gäller behandling av samma personuppgiftsansvarige eller personuppgiftsbiträde pågår i en domstol i en annan medlemsstat får alla andra behöriga domstolar än den där förfarandena först inleddes vilandeförklara förfarandena.
3. Om dessa förfaranden prövas i första instans får varje domstol, utom den vid vilken förfarandena först inleddes, också förklara sig obehörig på begäran av en av parterna, om den domstol vid vilken förfarandena först inleddes är behörig att pröva de berörda förfarandena och dess lagstiftning tillåter förening av dessa.

*Artikel 82***Ansvar och rätt till ersättning**

1. Varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av denna förordning ska ha rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den uppkomna skadan.
2. Varje personuppgiftsansvarig som medverkat vid behandlingen ska ansvara för skada som orsakats av behandling som strider mot denna förordning. Ett personuppgiftsbiträde ska ansvara för skada uppkommen till följd av behandlingen endast om denne inte har fullgjort de skyldigheter i denna förordning som specifikt riktar sig till personuppgiftsbiträden eller agerat utanför eller i strid med den personuppgiftsansvariges lagenliga anvisningar.
3. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska undgå ansvar enligt punkt 2 om den visar att den inte på något sätt är ansvarig för den händelse som orsakade skadan.
4. Om mer än en personuppgiftsansvarig eller ett personuppgiftsbiträde, eller både en personuppgiftsansvarig och ett personuppgiftsbiträde, har medverkat vid samma behandling, och om de enligt punkterna 2 och 3 är ansvariga för eventuell skada som behandlingen orsakat ska varje personuppgiftsansvarig eller personuppgiftsbiträde hållas ansvarig för hela skadan för att säkerställa att den registrerade får effektiv ersättning.
5. Om en personuppgiftsansvarig eller ett personuppgiftsbiträde, i enlighet med punkt 4, har betalat full ersättning för den skada som orsakats ska den personuppgiftsansvarige eller personuppgiftsbiträdet ha rätt att från de andra personuppgiftsansvariga eller personuppgiftsbiträdena som medverkat vid samma behandling återkräva den del av ersättningen som motsvarar deras del av ansvaret för skadan i enlighet med de villkor som fastställs i punkt 2.

6. Domstolsförfaranden för utövande av rätten till ersättning ska tas upp vid de domstolar som är behöriga enligt den nationella rätten i den medlemsstat som avses i artikel 79.2.

Artikel 83

Allmänna villkor för påförande av administrativa sanktionsavgifter

1. Varje tillsynsmyndighet ska säkerställa att påförande av administrativa sanktionsavgifter i enlighet med denna artikel för sådana överträdelser av denna förordning som avses i punkterna 4, 5 och 6 i varje enskilt fall är effektivt, proportionellt och avskräckande.

2. Administrativa sanktionsavgifter ska, beroende på omständigheterna i det enskilda fallet, påföras utöver eller i stället för de åtgärder som avses i artikel 58.2 a–h och j. Vid beslut om huruvida administrativa sanktionsavgifter ska påföras och om beloppet för de administrativa sanktionsavgifterna i varje enskilt fall ska vederbörlig hänsyn tas till följande:

- a) Överträdelsens karaktär, svårighetsgrad och varaktighet med beaktande av den aktuella uppgiftsbehandlings karaktär, omfattning eller syfte samt antalet berörda registrerade och den skada som de har lidit.
- b) Om överträdelsen skett med uppsåt eller genom oaktsamhet.
- c) De åtgärder som den personuppgiftsansvarige eller personuppgiftsbiträdet har vidtagit för att lindra den skada som de registrerade har lidit.
- d) Graden av ansvar hos den personuppgiftsansvarige eller personuppgiftsbiträdet med beaktande av de tekniska och organisatoriska åtgärder som genomförts av dem i enlighet med artiklarna 25 och 32.
- e) Eventuella relevanta tidigare överträdelser som den personuppgiftsansvarige eller personuppgiftsbiträdet gjort sig skyldig till.
- f) Graden av samarbete med tillsynsmyndigheten för att komma till rätta med överträdelsen och minska dess potentiella negativa effekter.
- g) De kategorier av personuppgifter som påverkas av överträdelsen.
- h) Det sätt på vilket överträdelsen kom till tillsynsmyndighetens kännedom, särskilt huruvida och i vilken omfattning den personuppgiftsansvarige eller personuppgiftsbiträdet anmälde överträdelsen.
- i) När åtgärder enligt artikel 58.2 tidigare har förordnats mot den berörda personuppgiftsansvarige eller personuppgiftsbiträdet vad gäller samma sakfråga, efterlevnad av dessa åtgärder.
- j) Tillämpandet av godkända uppförandekoder i enlighet med artikel 40 eller godkända certifieringsmekanismer i enlighet med artikel 42.
- k) Eventuell annan försvårande eller förmildrande faktor som är tillämplig på omständigheterna i fallet, såsom ekonomisk vinst som görs eller förlust som undviks, direkt eller indirekt, genom överträdelsen.

3. Om en personuppgiftsansvarig eller ett personuppgiftsbiträde, med avseende på en och samma eller sammankopplade uppgiftsbehandlingar, uppsåtligen eller av oaktsamhet överträder flera av bestämmelserna i denna förordning får den administrativa sanktionsavgiftens totala belopp inte överstiga det belopp som fastställs för den allvarligaste överträdelsen.

4. Vid överträdelser av följande bestämmelser ska det i enlighet med punkt 2 påföras administrativa sanktionsavgifter på upp till 10 000 000 EUR eller, om det gäller ett företag, på upp till 2 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

- a) Personuppgiftsansvarigas och personuppgiftsbitrådets skyldigheter enligt artiklarna 8, 11, 25–39, 42 och 43.
- b) Certifieringsorganets skyldigheter enligt artiklarna 42 och 43.
- c) Övervakningsorganets skyldigheter enligt artikel 41.4.

5. Vid överträdelser av följande bestämmelser ska det i enlighet med punkt 2 påföras administrativa sanktionsavgifter på upp till 20 000 000 EUR eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

- a) De grundläggande principerna för behandling, inklusive villkoren för samtycke, enligt artiklarna 5, 6, 7 och 9.
- b) Registrerades rättigheter enligt artiklarna 12–22.
- c) Överföring av personuppgifter till en mottagare i ett tredjeland eller en internationell organisation enligt artiklarna 44–49.
- d) Alla skyldigheter som följer av medlemsstaternas lagstiftning som antagits på grundval av kapitel IX.
- e) Underlåtenhet att rätta sig efter ett föreläggande eller en tillfällig eller permanent begränsning av behandling av uppgifter eller ett beslut om att avbryta uppgiftsflödena som meddelats av tillsynsmyndigheten i enlighet med artikel 58.2 eller underlåtenhet att ge tillgång till uppgifter i strid med artikel 58.1.

6. Vid underlåtenhet att rätta sig efter ett föreläggande från tillsynsmyndigheten i enlighet med artikel 58.2 ska det i enlighet med punkt 2 i den här artikeln påföras administrativa sanktionsavgifter på upp till 20 000 000 EUR eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

7. Utan att det påverkar tillsynsmyndigheternas korrigerande befogenheter enligt artikel 58.2 får varje medlemsstat fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter och organ som är inrättade i medlemsstaten.

8. Tillsynsmyndighetens utövande av sina befogenheter enligt denna artikel ska omfattas av lämpliga rättssäkerhetsgarantier i enlighet med unionsrätten och medlemsstaternas nationella rätt, inbegripet effektiva rättsmedel och rättssäkerhet.

9. Om det i medlemsstatens rättssystem inte finns några föreskrifter om administrativa sanktionsavgifter får den här artikeln tillämpas så att förfarandet inleds av den behöriga tillsynsmyndigheten och sanktionsavgifterna sedan utdöms av behörig nationell domstol, varvid det säkerställs att rättsmedlen är effektiva och har motsvarande verkan som de administrativa sanktionsavgifter som påförs av tillsynsmyndigheter. De sanktionsavgifter som påförs ska i alla händelser vara effektiva, proportionella och avskräckande. Dessa medlemsstater ska till kommissionen anmäla de bestämmelser i deras lagstiftning som de antar i enlighet med denna punkt senast den 25 maj 2018, samt utan dröjsmål anmäla eventuell senare ändringslagstiftning eller ändringar som berör dem.

Artikel 84

Sanktioner

1. Medlemsstaterna ska fastställa regler om andra sanktioner för överträdelser av denna förordning, särskilt för överträdelser som inte är föremål för administrativa sanktionsavgifter enligt artikel 83, och vidta alla nödvändiga åtgärder för att säkerställa att de genomförs. Dessa sanktioner ska vara effektiva, proportionella och avskräckande.

2. Varje medlemsstat ska till kommissionen anmäla de bestämmelser i sin lagstiftning som den antar i enlighet med punkt 1 senast den 25 maj 2018, samt utan dröjsmål anmäla eventuella senare ändringar som berör dem.

KAPITEL IX

Bestämmelser om särskilda behandlingssituationer

Artikel 85

Behandling och yttrande- och informationsfriheten

1. Medlemsstaterna ska i lag förena rätten till integritet i enlighet med denna förordning med yttrande- och informationsfriheten, inbegripet behandling som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

2. Medlemsstaterna ska, för behandling som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande, fastställa undantag eller avvikelser från kapitel II (principer), kapitel III (den registrerades rättigheter), kapitel IV (personuppgiftsansvarig och personuppgiftsbiträde), kapitel V (överföring av personuppgifter till tredjeländer eller internationella organisationer), kapitel VI (oberoende tillsynsmyndigheter), kapitel VII (samarbete och enhetlighet) och kapitel IX (särskilda situationer vid behandling av personuppgifter) om dessa är nödvändiga för att förena rätten till integritet med yttrande- och informationsfriheten.

3. Varje medlemsstat ska till kommissionen anmäla de bestämmelser i sin lagstiftning som den antagit i enlighet med punkt 2, samt utan dröjsmål anmäla eventuell senare ändringslagstiftning eller ändringar som berör dem.

Artikel 86

Behandling och allmänhetens tillgång till allmänna handlingar

Personuppgifter i allmänna handlingar som förvaras av en myndighet eller ett offentligt organ eller ett privat organ för utförande av en uppgift av allmänt intresse får lämnas ut av myndigheten eller organet i enlighet med den unionsrätt eller den medlemsstats nationella rätt som myndigheten eller det offentliga organet omfattas av, för att jämka samman allmänhetens rätt att få tillgång till allmänna handlingar med rätten till skydd av personuppgifter i enlighet med denna förordning.

Artikel 87

Behandling av nationella identifikationsnummer

Medlemsstaterna får närmare bestämma på vilka särskilda villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas. Ett nationellt identifikationsnummer eller ett annat vedertaget sätt för identifiering ska i sådana fall endast användas med iakttagande av lämpliga skyddsåtgärder för de registrerades rättigheter och friheter enligt denna förordning.

Artikel 88

Behandling i anställningsförhållanden

1. Medlemsstaterna får i lag eller i kollektivavtal fastställa mer specifika regler för att säkerställa skyddet av rättigheter och friheter vid behandling av anställdas personuppgifter i anställningsförhållanden, särskilt när det gäller rekrytering, genomförande av anställningsavtalet inklusive befrielse från i lag eller kollektivavtal stadgade skyldigheter, ledning, planering och organisering av arbetet, jämställdhet och mångfald i arbetslivet, hälsa och säkerhet på arbetsplatsen samt skydd av arbetsgivarens eller kundens egendom men också när det gäller att såväl kollektivt som individuellt utöva och komma i åtnjutande av rättigheter och förmåner som är knutna till anställningen samt att avsluta anställningsförhållandet.

2. Dessa regler ska innehålla lämpliga och specifika åtgärder för att skydda den registrerades mänskliga värdighet, berättigade intressen och grundläggande rättigheter, varvid hänsyn särskilt ska tas till insyn i behandlingen, överföring av personuppgifter inom en koncern eller en grupp av företag som deltar i gemensam ekonomisk verksamhet samt övervakningssystem på arbetsplatsen.

3. Varje medlemsstat ska till kommissionen anmäla de bestämmelser i sin lagstiftning som den antar i enlighet med punkt 1 senast den 25 maj 2018, samt utan dröjsmål anmäla eventuella senare ändringar som berör dem.

Artikel 89

Skyddsåtgärder och undantag för behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål

1. Behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål ska omfattas av lämpliga skyddsåtgärder i enlighet med denna förordning för den registrerades rättigheter och friheter. Skyddsåtgärderna ska säkerställa att tekniska och organisatoriska åtgärder har införts för att se till att särskilt

principen om uppgiftsminimering iakttas. Dessa åtgärder får inbegripa pseudonymisering, under förutsättning att dessa ändamål kan uppfyllas på det sättet. När dessa ändamål kan uppfyllas genom vidare behandling av uppgifter som inte medger eller inte längre medger identifiering av de registrerade ska dessa ändamål uppfyllas på det sättet.

2. Om personuppgifter behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål får det i unionsrätten eller i medlemsstaternas nationella rätt föreskrivas undantag från de rättigheter som avses i artiklarna 15, 16, 18 och 21 med förbehåll för de villkor och skyddsåtgärder som avses i punkt 1 i den här artikeln i den utsträckning som sådana rättigheter sannolikt kommer att göra det omöjligt eller mycket svårare att uppfylla de särskilda ändamålen, och sådana undantag krävs för att uppnå dessa ändamål.

3. Om personuppgifter behandlas för arkivändamål av allmänt intresse får det i unionsrätten eller i medlemsstaternas nationella rätt föreskrivas om undantag från de rättigheter som avses i artiklarna 15, 16, 18, 19, 20 och 21 med förbehåll för de villkor och skyddsåtgärder som avses i punkt 1 i den här artikeln i den utsträckning som sådana rättigheter sannolikt kommer att göra det omöjligt eller mycket svårare att uppfylla de särskilda ändamålen, och sådana undantag krävs för att uppnå dessa ändamål.

4. Om behandling enligt punkterna 2 och 3 samtidigt har andra ändamål, ska undantagen endast tillämpas på behandling för de ändamål som avses i dessa punkter.

Artikel 90

Tystnadsplikt

1. Medlemsstaterna får anta särskilda bestämmelser för att fastställa tillsynsmyndigheternas befogenheter enligt artikel 58.1 e och f gentemot personuppgiftsansvariga eller personuppgiftsbiträden som enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställts av behöriga nationella organ omfattas av tystnadsplikt eller andra motsvarande former av förbud mot att lämna ut uppgifter, om det är nödvändigt och står i proportion till vad som behövs för att förena rätten till skydd för personuppgifter och tystnadsplikten. Dessa bestämmelser ska endast tillämpas med avseende på personuppgifter som den personuppgiftsansvarige eller personuppgiftsbiträdet har erhållit i samband med en verksamhet som omfattas av denna tystnadsplikt.

2. Varje medlemsstat ska till kommissionen anmäla de bestämmelser den har antagit i enlighet med punkt 1 senast den 25 maj 2018, samt utan dröjsmål anmäla eventuella ändringar som berör dem.

Artikel 91

Befintliga bestämmelser om dataskydd inom kyrkor och religiösa samfund

1. Om kyrkor och religiösa samfund eller gemenskaper i en medlemsstat vid tidpunkten för ikraftträdandet av denna förordning tillämpar övergripande bestämmelser om skyddet av fysiska personer i samband med behandling, får sådana befintliga bestämmelser fortsätta att tillämpas under förutsättning att de görs förenliga med denna förordning.

2. Kyrkor och religiösa samfund som tillämpar övergripande bestämmelser i enlighet med punkt 1 i denna artikel ska vara föremål för kontroll av en oberoende tillsynsmyndighet som kan vara specifik, förutsatt att den uppfyller de villkor som fastställs i kapitel VI i denna förordning.

KAPITEL X

Delegerade akter och genomförandeakter

Artikel 92

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artikel 12.8 och artikel 43.8 ska ges till kommissionen tills vidare från och med den 24 maj 2016.
3. Den delegering av befogenhet som avses i artikel 12.8 och artikel 43.8 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.
4. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.
5. En delegerad akt som antas enligt artikel 12.8 och artikel 43.8 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period av tre månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med tre månader på Europaparlamentets eller rådets initiativ.

Artikel 93

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.
2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.
3. När det hänvisas till denna punkt ska artikel 8 i förordning (EU) nr 182/2011, jämförd med artikel 5 i samma förordning, tillämpas.

KAPITEL XI

Slutbestämmelser

Artikel 94

Upphävande av direktiv 95/46/EG

1. Direktiv 95/46/EG ska upphöra att gälla med verkan från och med den 25 maj 2018.
2. Hänvisningar till det upphävda direktivet ska anses som hänvisningar till denna förordning. Hänvisningar till arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter, som inrättades genom artikel 29 i direktiv 95/46/EG, ska anses som hänvisningar till Europeiska dataskyddsstyrelsen, som inrättas genom denna förordning.

Artikel 95

Förhållande till direktiv 2002/58/EG

Denna förordning ska inte innebära några ytterligare förpliktelser för fysiska eller juridiska personer som behandlar personuppgifter inom ramen för tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät i unionen, när det gäller områden inom vilka de redan omfattas av särskilda skyldigheter för samma ändamål i enlighet med direktiv 2002/58/EG.

*Artikel 96***Förhållande till tidigare ingångna avtal**

De internationella avtal som rör överföring av personuppgifter till tredjeländer eller internationella organisationer som ingicks av medlemsstaterna före den 24 maj 2016 och som är förenliga med unionsrätten i dess lydelse innan detta datum, ska fortsätta att gälla tills de ändras, ersätts eller återkallas.

*Artikel 97***Kommissionsrapporter**

1. Senast den 25 maj 2020 och därefter vart fjärde år ska kommissionen överlämna en rapport om tillämpningen och översynen av denna förordning till Europaparlamentet och rådet.
2. Inom ramen för de utvärderingar och översyner som avses i punkt 1 ska kommissionen särskilt undersöka hur följande bestämmelser tillämpas och fungerar:
 - a) Kapitel V om överföring av personuppgifter till tredjeländer och internationella organisationer, särskilt när det gäller beslut som antagits enligt artikel 45.3 i den här förordningen och beslut som antagits på grundval av artikel 25.6 i direktiv 95/46/EG.
 - b) Kapitel VII om samarbete och enhetlighet.
3. Med avseende på tillämpningen av punkt 1 får kommissionen begära information från medlemsstaterna och tillsynsmyndigheterna.
4. Kommissionen ska när den utför de utvärderingar och översyner som avses i punkterna 1 och 2 ta hänsyn till ståndpunkter och slutsatser från Europaparlamentet, rådet och andra relevanta organ och källor.
5. Kommissionen ska om nödvändigt överlämna lämpliga förslag om ändring av denna förordning, med särskild hänsyn till informationsteknikens utveckling och mot bakgrund av tendenserna inom informationsområdet.

*Artikel 98***Översyn av andra unionsrättsakter om dataskydd**

Kommissionen ska, om så är lämpligt, lägga fram lagstiftningsförslag i syfte att ändra andra unionsrättsakter om skydd av personuppgifter, för att säkerställa ett enhetligt och konsekvent skydd för fysiska personer med avseende på behandling. Detta gäller i synnerhet bestämmelserna om skyddet för fysiska personer i samband med behandling som utförs av unionens institutioner, organ och byråer samt om det fria flödet av sådana uppgifter.

*Artikel 99***Ikraftträdande och tillämpning**

1. Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.
2. Den ska tillämpas från och med den 25 maj 2018.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 27 april 2016.

På Europaparlamentets vägnar

M. SCHULZ

Ordförande

På rådets vägnar

J.A. HENNIS-PLASSCHAERT

Ordförande

Statens offentliga utredningar 2017

Kronologisk förteckning

1. För Sveriges landsbygder
– en sammanhållen politik för
arbete, hållbar tillväxt och välfärd. N.
2. Kraftsamling för framtidens energi. M.
3. Karens för statsråd och statssekreterare.
Fi.
4. För en god och jämlik hälsa.
En utveckling av det
folkhälsopolitiska ramverket. S.
5. Svensk social trygghet i en
globaliserad värld. Del 1 och 2. S.
6. Se barnet! Ju.
7. Straffprocessens ramar och
domstolens beslutsunderlag
i brottmål – en bättre hantering av
stora mål. Ju.
8. Kunskapsläget på kärnavfallsområdet 2017.
Kärnavfallet – en fråga i ständigt
förändring. M.
9. Det handlar om oss.
– unga som varken arbetar eller studerar. U.
10. Ny ordning för att främja god sed
och hantera oredlighet i forskning. U.
11. Vägs katt. Volym 1 och 2. Fi.
12. Att ta emot människor på flykt.
Sverige hösten 2015. Ju.
13. Finansiering av infrastruktur med
privat kapital? Fi.
14. Migrationsärenden
vid utlandsmyndigheterna. Ju.
15. Kvalitet och säkerhet
på apoteksmarknaden. S.
16. Sverige i Afghanistan 2002–2014. UD.
17. Om oskuldspresumtionen och rätten att
närvara vid rättegången. Genomförande
av EU:s oskuldspresumtionsdirektiv. Ju.
18. En nationell strategi för validering. U.
19. Uppdrag: Samverkan. Steg på vägen
mot fördjupad lokal samverkan
för unga arbetslösa. A.
20. Tillträde för nybörjare – ett öppnare
och enklare system för tillträde till
högskoleutbildning. U.
21. Läs mig! Nationell kvalitetsplan för
vård och omsorg om äldre personer.
Del 1 och 2. S.
22. Från värdekedja till värdecykel – så får
Sverige en mer cirkulär ekonomi. M.
23. digitalforvaltning.nu. Fi.
24. Ett arbetsliv i förändring – hur
påverkas ansvaret för arbetsmiljön? A.
25. Samlad kunskap – stärkt
handläggning. S.
26. Delningsekonomi. På användarnas
villkor. Fi.
27. Vissa frågor inom fastighets- och
stämpelskatteområdet. Fi.
28. Ett nationellt centrum för kunskap
om och utvärdering av arbetsmiljö. A.
29. Brottdatalag. Ju.
30. En omreglerad spelmarknad.
Del 1 och 2. Fi.
31. Stärkt konsumentskydd
på bostadsrättsmarknaden. Ju.
32. Substitution i Centrum
– stärkt konkurrenskraft med
kemikaliesmarta lösningar. M.
33. Stärkt ställning för hyresgäster. Ju.
34. Ekologisk kompensation – Åtgärder
för att motverka nettoförluster av
biologisk mångfald och ekosystem-
tjänster, samtidigt som behovet av
markexploatering tillgodoses. M.
35. Samling för skolan. Nationell strategi
för kunskap och likvärdighet. U.
36. Informationssäkerhet för
samhällsviktiga och digitala tjänster.
Ju.
37. Kvalificerad välfärdsbrottslighet
– förebygga, förhindra, upptäcka och
beivra. Ju.
38. Kvalitet i välfärden – bättre
upphandling och uppföljning. Fi.
39. Ny dataskyddslag. Kompletterande
bestämmelser till EU:s dataskydds-
förordning. Ju.

Statens offentliga utredningar 2017

Systematisk förteckning

Arbetsmarknadsdepartementet

- Uppdrag: Samverkan. Steg på vägen mot fördjupad lokal samverkan för unga arbetslösa. [19]
- Ett arbetsliv i förändring – hur påverkas ansvaret för arbetsmiljön? [24]
- Ett nationellt centrum för kunskap om och utvärdering av arbetsmiljö. [28]

Finansdepartementet

- Karens för statsråd och statssekreterare. [3]
- Vägs katt. Volym 1 och 2. [11]
- Finansiering av infrastruktur med privat kapital? [13]
- digitalforvaltning.nu. [23]
- Delningsekonomi. På användarnas villkor. [26]
- Vissa frågor inom fastighets- och stämpel-skatteområdet. [27]
- En omreglerad spelmarknad. Del 1 och 2. [30]
- Kvalitet i välfärden – bättre upphandling och uppföljning. [38]

Justitiedepartementet

- Se barnet! [6]
- Straffprocessens ramar och domstolens beslutsunderlag i brottmål – en bättre hantering av stora mål. [7]
- Att ta emot människor på flykt. Sverige hösten 2015. [12]
- Migrationsärenden vid utlandsmyndigheterna. [14]
- Om oskuldspresumtionen och rätten att närvara vid rättegången. Genomförande av EU:s oskuldspresumtionsdirektiv. [17]
- Brottsdatalag. [29]
- Stärkt konsumentskydd på bostadsrättsmarknaden. [31]
- Stärkt ställning för hyresgäster. [33]

Informationssäkerhet för samhällsviktiga och digitala tjänster. [36]

Kvalificerad välfärdsbrottslighet – förebygga, förhindra, upptäcka och beivra. [37]

Ny dataskyddslag. Kompletterande bestämmelser till EU:s dataskyddsförordning. [39]

Miljö- och energidepartementet

- Kraftsamling för framtidens energi. [2]
- Kunskapsläget på kärnavfallsområdet 2017. Kärnavfallet – en fråga i ständig förändring. [8]
- Från värdekedja till värdecykel – så får Sverige en mer cirkulär ekonomi. [22]
- Substitution i Centrum – stärkt konkurrenskraft med kemikaliesmarta lösningar. [32]
- Ekologisk kompensation – Åtgärder för att motverka nettoförluster av biologisk mångfald och ekosystemtjänster, samtidigt som behovet av markexploatering tillgodoses. [34]

Näringsdepartementet

För Sveriges landsbygder – en sammanhållen politik för arbete, hållbar tillväxt och välfärd. [1]

Socialdepartementet

- För en god och jämlik hälsa. En utveckling av det folkhälsopolitiska ramverket. [4]
- Svensk social trygghet i en globaliserad värld. Del 1 och 2. [5]
- Kvalitet och säkerhet på apoteksmarknaden. [15]
- Läs mig! Nationell kvalitetsplan för vård och omsorg om äldre personer. Del 1 och 2. [21]
- Samlad kunskap – stärkt handläggning. [25]

Utbildningsdepartementet

Det handlar om oss.

– unga som varken arbetar eller studerar. [9]

Ny ordning för att främja god sed
och hantera oredlighet i forskning. [10]

En nationell strategi för validering [18]

Tillträde för nybörjare – ett öppnare och
enklare system för tillträde till hög-
skoleutbildning. [20]

Samling för skolan.

Nationell strategi för kunskap och
likvärdighet. [35]

Utrikesdepartementet

Sverige i Afghanistan 2002–2014. [16]