

# En omarbetad utlänningsdatalag

## Anpassning till EU:s dataskyddsförordning



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](mailto:kundservice@wolterskluwer.se)  
Webbplats: [wolterskluwer.se/offentligapublikationer](http://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](http://regeringen.se/remisser)

Omslag: Regeringskansliets standard  
Tryck: Elanders Sverige AB, Stockholm 2017

ISBN 978-91-38-24678-8  
ISSN 0284-6012

# Förord

Chefen för Justitiedepartementet beslutade den 7 april 2017 att ge mig i tilläggsuppdrag att inom ramen för uppdraget Ju 2016:G biträda Justitiedepartementet med att lämna förslag på de författningsändringar som behövs för att komplettera EU:s dataskyddsförordning i utlänningsdatalagen (2016:27) och utlänningsdataförordningen (2016:30).

Tf. rådmannen Nina Stierna har biträtt mig som sekreterare i uppdraget.

Vi får härmed överlämna promemorian *En omarbetad utlänningsdatalag* (Ds 2017:45).

Uppdraget är med detta slutfört.

Jönköping i september 2017

Peder Liljeqvist

/ Nina Stierna



# Innehåll

<b>Vissa förkortningar .....</b>	<b>11</b>
<b>Sammanfattning .....</b>	<b>13</b>
<b>1 Författningsförslag.....</b>	<b>17</b>
1.1 Förslag till lag om ändring i utlänningsdatalagen (2016:27) .....	17
1.2 Förslag till förordning om ändring i utlänningsdataförordningen (2016:30).....	27
<b>2 Uppdraget och dess genomförande.....</b>	<b>29</b>
2.1 Uppdraget.....	29
2.2 Avgränsningar .....	29
2.3 Uppdragets genomförande.....	30
2.4 Promemorians disposition .....	30
<b>3 Gällande rätt.....</b>	<b>33</b>
3.1 FN.....	33
3.2 OECD .....	33
3.3 Europarådet .....	34
3.3.1 Europakonventionen.....	34
3.3.2 Dataskyddskonventionen .....	34
3.4 EU.....	35
3.4.1 Stadgan .....	35

3.4.2	Dataskyddsdirektivet och dataskyddsrambeslutet.....	35
3.5	Svensk rätt.....	36
3.5.1	Regeringsformen.....	36
3.5.2	Personuppgiftslagen.....	37
3.6	Registerförfattningar för utlännings- och medborgarskapslagstiftningen .....	37
<b>4</b>	<b>Nya regelverk för personuppgiftsbehandling.....</b>	<b>41</b>
4.1	EU:s dataskyddsreform.....	41
4.1.1	Dataskyddsförordningen.....	41
4.1.2	2016 års dataskyddsdirektiv.....	42
4.2	Två nya svenska regelverk för personuppgiftsbehandling.....	43
<b>5</b>	<b>Nationella registerförfattningar .....</b>	<b>47</b>
5.1	Registerförfattningarnas förenlighet med dataskyddsförordningen .....	47
5.2	Allmänna principer för behandling av personuppgifter .....	49
5.3	Bedömning.....	50
<b>6</b>	<b>Rättslig grund för personuppgiftsbehandlingen inom tillämpningsområdet .....</b>	<b>53</b>
6.1	Dataskyddslagen.....	55
6.2	Myndighetsutövning, uppgift av allmänt intresse eller rättslig förpliktelse?.....	56
6.2.1	Uppgift av allmänt intresse.....	56
6.2.2	Myndighetsutövning.....	57
6.2.3	Rättslig förpliktelse.....	59
6.3	Den rättsliga grunden finns i artikel 6.1 c och e i dataskyddsförordningen .....	60
6.3.1	Myndigheternas uppdrag på utlännings- och medborgarskapsområdet.....	60
6.3.2	Bedömning .....	61

<b>7</b>	<b>Syfte och tillämpningsområde.....</b>	<b>69</b>
7.1	Lagens syfte.....	69
7.2	Verksamhet som omfattas av tillämpningsområdet.....	70
7.2.1	Migrationsverkets och utlandsmyndigheternas verksamhet.....	70
7.2.2	Polismyndighetens verksamhet.....	72
7.2.3	Avgränsning mot direktivsstyrd verksamhet.....	73
7.2.4	Bedömning.....	74
7.3	Avgränsningar för tillämpningsområdet.....	76
7.3.1	Lagen om Schengens informationssystem, Viseringskodexen och Eurodac-förordningen.....	76
7.3.2	Lagen om passagerarregister.....	78
7.3.3	VIS-förordningen.....	79
7.4	Automatiserad behandling och manuella register.....	83
<b>8</b>	<b>Ändamålsbestämmelser .....</b>	<b>87</b>
8.1	Primära ändamålsbestämmelser.....	87
8.1.1	Rättslig reglering.....	87
8.1.2	Tidigare förarbeten.....	88
8.2	Sekundära ändamålsbestämmelser.....	92
8.2.1	Rättslig reglering.....	92
8.2.2	Tidigare förarbeten.....	93
8.3	Ett uttryckligt angivet och tydligt ändamål.....	95
8.4	Finalitetsprincipen.....	95
8.5	Precisering av rättslig grund eller ändamålsbestämmelser?.....	97
8.6	Bedömning.....	98
8.6.1	Ändamålen för behandling bör uttryckligen anges.....	98
8.6.2	Tillräckligt tydliga och specifika ändamål.....	100
8.6.3	Uppgifter som har behandlats enligt brottsdatalogen.....	102
8.6.4	Hänvisningen till finalitetsprincipen.....	103

<b>9</b>	<b>Förhållandet till annan lagstiftning .....</b>	<b>105</b>
9.1	Förhållandet till personuppgiftslagen .....	105
9.2	Förhållandet till dataskyddsförordningen .....	105
9.3	Förhållandet till dataskyddslagen .....	108
9.4	Befintliga hänvisningar till personuppgiftslagen och hänvisningar till dataskyddslagen .....	109
9.4.1	Definitioner .....	109
9.4.2	Förhållandet till offentlighetsprincipen.....	109
9.4.3	Grundläggande krav på behandling av personuppgifter .....	110
9.4.4	Behandling av personnummer och samordningsnummer .....	110
9.4.5	Information till den registrerade och rättelse.....	111
9.4.6	Säkerhet vid behandlingen .....	111
9.4.7	Överföring till tredje land.....	111
9.4.8	Personuppgiftsombud och förhandskontroll.....	112
9.4.9	Upplysningar till allmänheten om vissa behandlingar .....	112
9.4.10	Tillsynsmyndighetens handläggning och beslut.....	113
9.4.11	Skadestånd .....	118
9.4.12	Överklagande .....	119
9.4.13	Förhållandet till tryck- och yttrandefriheten .....	119
9.4.14	Sanktionsavgifter.....	120
<b>10</b>	<b>Personuppgiftsansvaret .....</b>	<b>123</b>
<b>11</b>	<b>Dataskyddsombud.....</b>	<b>125</b>
11.1	1995 års dataskyddsdirektiv, personuppgiftslagen och utlänningsdatalagen .....	125
11.2	Dataskyddsförordningen .....	126
11.2.1	Myndigheter ska utse dataskyddsombud .....	126
11.2.2	Dataskyddsombudets ställning, uppgifter m.m. ....	127
11.3	Bedömning.....	129



11.3.1	Dataskyddssombudet – ”internrevisor” med något utökat uppdrag .....	129
11.3.2	Skyldigheten att utse dataskyddssombud och ombudets uppgifter framgår av dataskyddsförordningen .....	131
11.3.3	Tystnadsplikt för dataskyddssombudet.....	133
<b>12</b>	<b>Känsliga personuppgifter och sökbegränsningar .....</b>	<b>135</b>
12.1	Känsliga personuppgifter.....	135
12.1.1	Dataskyddsförordningen och 1995 års dataskyddsdirektiv.....	135
12.1.2	Dataskyddslagen.....	136
12.1.3	Utlänningsdatalagens allmänna bestämmelser.....	137
12.1.4	Migrationsverkets register över fingeravtryck och fotografier .....	138
12.1.5	Bedömning.....	139
12.2	Sökbegränsningar.....	144
12.2.1	Utlänningsdatalagen och dataskyddslagen .....	144
12.2.2	Bedömning.....	145
<b>13</b>	<b>Tillgången till personuppgifter .....</b>	<b>149</b>
13.1	Utlänningsdatalagen och utlänningsdataförordningen .....	149
13.2	Bedömning .....	150
<b>14</b>	<b>Den registrerades rättigheter.....</b>	<b>153</b>
14.1	Inledande kommentar.....	153
14.2	En generell möjlighet till undantag.....	154
14.3	Information när personuppgifter samlas in från den registrerade .....	155
14.3.1	Utlänningsdatalagen och personuppgiftslagen....	155
14.3.2	Dataskyddsförordningen och dataskyddslagen...	155
14.3.3	Bedömning.....	156
14.4	Information när personuppgifter samlas in från någon annan än den registrerade .....	158
14.4.1	Utlänningsdatalagen och personuppgiftslagen....	158

14.4.2	Dataskyddsförordningen.....	159
14.4.3	Bedömning .....	159
14.5	Information efter begäran.....	160
14.5.1	Utlänningsdatalagen och personuppgiftslagen ...	160
14.5.2	Dataskyddsförordningen och dataskyddslagen ..	161
14.5.3	Bedömning .....	162
14.6	Rättelse och radering samt rätt att göra invändningar och begära begränsning av behandling.....	163
14.6.1	Utlänningsdatalagen, personuppgiftslagen och 1995 års dataskyddsdirektiv.....	163
14.6.2	Dataskyddsförordningen.....	165
14.6.3	Bedömning .....	167
14.7	Automatiserade beslut.....	172
14.8	Skadestånd.....	174
14.8.1	Utlänningsdatalagen och personuppgiftslagen ...	174
14.8.2	Dataskyddsförordningen.....	174
14.8.3	Dataskyddslagen .....	175
14.8.4	Bedömning .....	175
14.9	Information om personuppgiftsincidenter .....	176
14.9.1	Dataskyddsförordningen.....	176
14.9.2	Bedömning .....	177
<b>15</b>	<b>Direktåtkomst och sekretessbrytande bestämmelser ....</b>	<b>179</b>
15.1	Direktåtkomst .....	179
15.1.1	Proportionalitetsbedömning .....	179
15.1.2	Innebörden av direktåtkomst.....	180
15.1.3	Utlänningsdatalagen och utlänningsdataförordningen .....	182
15.2	Sekretessbrytande bestämmelser .....	184
15.3	Bedömning.....	184
<b>16</b>	<b>Tredjelandsoverföringar .....</b>	<b>187</b>
16.1	Utlänningsdatalagen och personuppgiftslagen.....	187
16.2	Dataskyddsförordningen .....	188

16.3	Bedömning .....	189
<b>17</b>	<b>Bevarande, avskiljande och gallring av personuppgifter .....</b>	<b>191</b>
17.1	Bevarande av personuppgifter .....	191
17.1.1	Utlänningsdatalagen och personuppgiftslagen ....	191
17.1.2	Dataskyddsförordningen .....	193
17.1.3	Dataskyddslagen .....	195
17.1.4	Bedömning .....	196
17.2	Avskiljande av personuppgifter.....	202
17.2.1	Utlänningsdatalagen och utlänningsdataförordningen.....	202
17.2.2	Bedömning.....	203
17.3	Gallring av personuppgifter.....	205
17.3.1	Arkivreglerna i korthet.....	205
17.3.2	Utlänningsdatalagen och utlänningsdataförordningen.....	205
17.3.3	Bedömning.....	207
<b>18</b>	<b>Föreskriftsrätten .....</b>	<b>211</b>
18.1	Utlänningsdatalagen och utlänningsdataförordningen .....	211
18.2	Bedömning .....	212
<b>19</b>	<b>Överklagandebestämmelser .....</b>	<b>213</b>
19.1	Utlänningsdatalagen och personuppgiftslagen .....	213
19.2	Dataskyddsförordningen och stadgan .....	213
19.3	Dataskyddslagen .....	215
19.3.1	Överklagande av en myndighets beslut.....	215
19.3.2	Dröjsmålstalan.....	216
19.3.3	Överklagande av tillsynsmyndighetens beslut.....	217
19.3.4	Beslut om enskilt organs behandling för arkivändamål .....	217
19.3.5	Uttömmande överklagandebestämmelser.....	218
19.4	Bedömning .....	218

<b>20</b>	<b>Övergångs- och ikraftträdandebestämmelser .....</b>	<b>223</b>
20.1	Två olika ikraftträdandedatum.....	223
20.2	Pågående ärenden .....	224
20.3	Beslut som har meddelats före ikraftträdandet.....	226
20.4	Skada som har orsakats före ikraftträdandet .....	228
20.5	Sanktioner mot överträdelser som har skett före ikraftträdandet .....	229
<b>21</b>	<b>Konsekvenser av förslagen .....</b>	<b>231</b>
21.1	Analysens omfattning och förslagets konsekvenser.....	231
21.2	Tillsynsmyndighetens handläggning och beslut samt sanktionsavgifter.....	232
<b>22</b>	<b>Författningskommentar .....</b>	<b>235</b>
22.1	Förslaget till lag om ändring i utlänningsdatalagen (2016:27) .....	235
22.2	Förslaget till förordning om ändring i utlänningsdataförordningen (2016:30) .....	243
Bilaga 1	Uppdraget .....	245
Bilaga 2	Konsoliderad version av utlänningsdatalagen enligt våra förslag.....	249
Bilaga 3	Europaparlamentets och rådets förordning (EU) 2016/679 .....	259

# Vissa förkortningar

1995 års dataskyddsdirektiv	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
2016 års dataskyddsdirektiv	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
a.a.	anfört arbete
a.prop.	anförd proposition
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)

dir.	direktiv
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./ff.	följande sida/sidor
FN	Förenta nationerna
HFD	Högsta förvaltningsdomstolens årsbok
NJA	Nytt juridiskt arkiv
OECD	Organisationen för ekonomiskt samarbete och utveckling
OSL	Offentlighets- och sekretesslagen (2009:400)
prop.	regeringens proposition
PuL	Personuppgiftslagen (1998:204)
RF	Regeringsformen
RÅ	Regeringsrättens årsbok
SOU	Statens offentliga utredningar
TF	Tryckfrihetsförordningen

# Sammanfattning

## Anpassningar till EU:s dataskyddsförordning

EU:s dataskyddsreform innebär att en ny dataskyddsförordning<sup>1</sup> kommer att utgöra grunden för generell personuppgiftsbehandling inom EU från och med den 25 maj 2018. Reformen omfattar även ett nytt direktiv med särregler för den personuppgiftsbehandling som utförs av behöriga myndigheter för bl.a. brottsbekämpning, lagföring och straffverkställighet.<sup>2</sup> Denna promemoria innehåller förslag till de författningsändringar som behövs i utlänningsdatalagen (2016:27) och utlänningsdataförordningen (2016:30) med anledning av dataskyddsförordningen.

## Tillämpningsområdet

Utlänningsdatalagen reglerar den personuppgiftsbehandling som utförs av Migrationsverket, Polismyndigheten och utlandsmyndigheterna i vissa utpekade verksamheter inom utlännings- och medborgarskapslagstiftningen. Tillämpningsområdet omfattar för närvarande dock inte den personuppgiftsbehandling som utförs i Polismyndighetens brottsbekämpande verksamhet. För att anpassa lagen till det nya regelverket för personuppgiftsbehandling föreslår vi att lagen inte ska gälla vid sådan behandling av personuppgifter som omfattas av brottsdatalagens tillämpningsområde. Vi föreslår

---

<sup>1</sup> Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för enskilda 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).

<sup>2</sup> 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.

också att det i utlänningsdatalagen ska klargöras att den lagen inte gäller när personuppgifter behandlas med stöd av lagen (2006:444) om passagerarregister. I övrigt ska lagens tillämpningsområde enligt vårt förslag kvarstå oförändrat. Dataskyddsförordningen ska tillämpas i Sverige som om den vore nationell rätt, men hindrar inte förekomsten av nationella registerförfattningar. Dessa kommer framöver dock endast att utgöra en komplettering till dataskyddsförordningen, vilket enligt vårt förslag ska klargöras i utlänningsdatalagen.

### **Grundläggande bestämmelser**

Den rättsliga grunden för den personuppgiftsbehandling som utförs inom utlänningsdatalagens tillämpningsområde utgörs enligt vår bedömning av att behandlingen är nödvändig för att fullgöra en rättslig förpliktelse, för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning.

Till allra största delen föranleder dataskyddsförordningen inte någon förändring av utlänningsdatalagens ändamålsbestämmelser. Vi föreslår dock att den hänvisning till finalitetsprincipen som finns i lagens sekundära ändamålsbestämmelser ska knyta an till dataskyddsförordningens bestämmelser i denna del. Vi föreslår också att det i utlänningsdatalagen klargörs att personuppgifter som behandlas eller har behandlats för lagens primära ändamål ska få behandlas om det behövs för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål, förutsatt att de säkerhetsåtgärder som framgår av artikel 89.1 i dataskyddsförordningen vidtas.

### **Övriga materiella bestämmelser**

Som vi nämnt ovan kommer utlänningsdatalagen framöver att utgöra en komplettering till dataskyddsförordningen. Det är således i förordningen som de grundläggande bestämmelserna om personuppgiftsbehandling kommer att finnas.

Till stora delar föranleder dataskyddsförordningen dock inga eller endast redaktionella ändringar av utlänningsdatalagen. Exempelvis kommer bestämmelserna om personuppgiftsansvar,



direktåtkomst, avskiljande och gallring att kunna kvarstå oförändrade i materiellt hänseende. Vi föreslår dock att bestämmelserna om behandling av känsliga personuppgifter anpassas till dataskyddsförordningen på så sätt att definitionen av vilka kategorier av personuppgifter som ska anses vara känsliga överensstämmer med dataskyddsförordningens begrepp. Detta innebär att även uppgifter om sexuell läggning, genetiska uppgifter och biometriska uppgifter för att entydigt identifiera en fysisk person tillkommer. Förändringen ska emellertid inte innebära några hinder mot att – på samma sätt som för närvarande – behandla personuppgifter som finns i Migrationsverkets register över fingeravtryck och fotografier.

Utlänningsdatalagens nuvarande bestämmelse om personuppgiftsombud kommer att ersättas med dataskyddsförordningens bestämmelser om skyldighet att utse dataskyddsombud. Förordningen är tydligare vad gäller ombudets ställning och uppgifter.

När dataskyddsförordningen börjar tillämpas ska personuppgiftslagen (1998:204) upphävas.<sup>3</sup> I enlighet med vad som tidigare gällt i förhållande till personuppgiftslagen föreslår vi att utlänningsdatalagen ska gälla i stället för den föreslagna lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (förkortad dataskyddslagen), som föreslås komplettera EU:s dataskyddsförordning på ett generellt plan i svensk rätt (se Data-skyddsutredningens betänkande [SOU 2017:39]). Det ska i utlänningsdatalagen särskilt anges vilka bestämmelser i dataskyddslagen som ska gälla inom tillämpningsområdet.

Genom hänvisningar till dataskyddslagens bestämmelser kommer stora delar av den tidigare regleringen för personuppgiftsbehandling att behållas. Det gäller bl.a. de aktuella myndigheternas rätt att behandla uppgifter om personnummer och samordningsnummer, begränsningen av den registrerades rätt till ett s.k. registerutdrag för uppgifter i löpande text eller minnesanteckningar samt rätten för myndigheterna att återanvända personuppgifter i arkiverade handlingar. Även de undantag som för närvarande finns från den registrerades rätt till information vid insamling av person-

---

<sup>3</sup> Se kommittédirektiv till Dataskyddsutredningen (Dir. 2016:15 s. 6).

uppgifter samt från rätten till ett registerutdrag kommer på detta sätt att upprätthållas.

Dataskyddsförordningen innehåller bestämmelser som i vissa fall ger den registrerade rätt till information om en inträffad personuppgiftsincident. För att säkerställa att den registrerade inte genom sådan information får del av uppgifter som det råder sekretess för gentemot honom eller henne, föreslår vi att det införs ett undantag från denna rättighet. Undantaget ska gälla om den personuppgiftsansvarige, enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning, inte får lämna ut uppgifter till den registrerade. De undantag från dataskyddsförordningens bestämmelser om den registrerades rättigheter som vi föreslagit får – tillsammans med de undantag som finns i dataskyddsförordningen – till följd att de aktuella myndigheternas verksamhet kan fortgå även om den registrerade utnyttjar sina rättigheter enligt dataskyddsförordningen. Handläggning av enskilda ärenden behöver inte avstanna, bevarande av handlingar kommer att vara möjlig, personuppgifter i avslutade och arkiverade ärenden kan fortsätta behandlas och allmänhetens tillgång till allmänna handlingar inskränks inte.

### **Tillsyn och överklagande**

Dataskyddsförordningen och förslaget till dataskyddslag kommer att förändra systemet för sanktioner vid otillåten personuppgiftsbehandling. Vi föreslår att dataskyddslagens bestämmelser om administrativa sanktionsavgifter mot myndigheter i tillämpliga delar ska gälla även på utlänningsdatalagens tillämpningsområde. Detsamma gäller för dataskyddslagens bestämmelser om tillsynsmyndighetens handläggning och beslut. Genom en hänvisning till dataskyddslagen ska det även klargöras att den rätt till skadestånd för registrerade som framgår av dataskyddsförordningen även gäller vid överträdelse av dataskyddslagens (i tillämpliga delar) och utlänningsdatalagens bestämmelser. Även dataskyddslagens överklagandebestämmelser kommer att gälla på utlänningsdatalagens tillämpningsområde.

# 1 Författningsförslag

## 1.1 Förslag till lag om ändring i utlänningsdatalagen (2016:27)

Härigenom föreskrivs i fråga om utlänningsdatalagen (2016:27)

- dels* att 10 § ska upphävas,
- dels* att rubriken närmast före 7 § ska utgå,
- dels* att nuvarande 14 § ska betecknas 15 a §,
- dels* att 3, 5–8, 13, 15, 17, 18, 20 och 21 §§ ska ha följande lydelse,
- dels* att rubriken närmast före nuvarande 14 § ska sättas närmast före 15 a §,
- dels* att det ska införas fyra nya paragrafer, 3 a, 6 a, 13 a och 18 a §§, och närmast före 6, 6 a och 18 a §§ nya rubriker av följande lydelse.

*Nuvarande lydelse*

*Föreslagen lydelse*

### 3 §

Denna lag gäller också vid behandling av personuppgifter i Polismyndighetens verksamhet som rör utlänningars inresa och vistelse i Sverige och utresa eller avlägsnande från Sverige *om verksamheten inte utgör brottsbekämpande verksamhet.*

Denna lag gäller också vid behandling av personuppgifter i Polismyndighetens verksamhet som rör utlänningars inresa och vistelse i Sverige och utresa eller avlägsnande från Sverige.

### 3 a §

*Denna lag gäller inte vid sådan behandling av personuppgifter som*

*omfattas av brottsdatalogens (2018:xx) tillämpningsområde.*

## 5 §

Denna lag gäller inte när personuppgifter behandlas med stöd av

1. lagen (2000:344) om Schengens informationssystem,

2. lagen (2006:444) om passagerarregister,

2. Europaparlamentets och rådets förordning (EG) nr 810/2009 av den 13 juli 2009 om införande av en gemenskapskodex om viseringar (viseringskodex), eller

3. Europaparlamentets och rådets förordning (EG) nr 810/2009 av den 13 juli 2009 om införande av en gemenskapskodex om viseringar (viseringskodex), eller

3. Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodac-uppgifter för brottsbekämpande ändamål, samt om ändring av förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet

4. Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodac-uppgifter för brottsbekämpande ändamål, samt om ändring av förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet

och rättvisa (omarbetning).

och rättvisa (omarbetning).

*Personuppgiftsbehandling enligt  
VIS-förordningen*

6 §

När personuppgifter behandlas med stöd av Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS-förordningen), gäller bestämmelserna i 28 och 48 §§ personuppgiftslagen (1998:204) om rättelse och skadestånd om inte något annat följer av VIS-förordningen. I övrigt är denna lag inte tillämplig när personuppgifter behandlas med stöd av VIS-förordningen.

När personuppgifter behandlas med stöd av Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS-förordningen) gäller, om inte något annat följer av VIS-förordningen, följande.

1. Den personuppgiftsansvarige är skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med VIS-förordningen. Den personuppgiftsansvarige ska också underrätta tredje man till vilken uppgifterna har lämnats ut om åtgärden, om den registrerade begär det eller om mera betydande skada eller olägenhet för den registrerade skulle kunna

*undvikas genom en underrättelse. Någon sådan underrättelse behöver dock inte lämnas, om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.*

*2. Den personuppgifts-ansvarige ska ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med VIS-förordningen har orsakat. Ersättningsskyldigheten kan i den utsträckning det är skäligt jämkas, om den personuppgiftsansvarige visar att felet inte berodde på honom eller henne.*

*I övrigt är denna lag inte tillämplig när personuppgifter behandlas med stöd av VIS-förordningen.*

### ***Förhållandet till annan lagstiftning***

#### ***6 a §***

*Denna lag innehåller kompletterande bestämmelser till 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 data-skyddsförordning).*

## 7 §

Om inte något annat anges i 8 §, gäller denna lag i stället för *personuppgiftslagen (1998:204)*.

Om inte något annat anges i 8 §, gäller denna lag i stället för *lagen (2018:xx) med kompletterande bestämmelser till EU:s dataskyddsförordning*.

8 §<sup>1</sup>

När personuppgifter behandlas enligt denna lag, eller enligt föreskrifter som har meddelats i anslutning till lagen, gäller följande bestämmelser i *personuppgiftslagen (1998:204)*:

1. 3 § om definitioner,
2. 8 § om förhållandet till offentlighetsprincipen,
3. 9 § om grundläggande krav på behandling av personuppgifter,
4. 22 § om behandling av personnummer,
5. 23 och 25–27 §§ om information till den registrerade,
6. 28 § om rättelse,
7. 30 och 31 §§ samt 32 § första stycket om säkerheten vid behandling,
8. 33–35 §§ om överföring av personuppgifter till tredjeland,
9. 38–41 §§ om personuppgiftsombud m.m.,
10. 42 § om upplysningar till allmänheten om vissa behandlingar,
11. 43 och 44 §§, 45 § första stycket och 47 § om tillsynsmyndighetens befogenheter,

När personuppgifter behandlas enligt denna lag, eller enligt föreskrifter som har meddelats i anslutning till lagen, gäller följande bestämmelser i *lagen (2018:xx) med kompletterande bestämmelser till EU:s dataskyddsförordning*:

1. 1 kap. 4 § första stycket om förhållandet till tryck- och yttrandefriheten,
2. 3 kap. 6 § första stycket om behandling av känsliga personuppgifter för arkivändamål av allmänt intresse,
3. 3 kap. 13 § om behandling av personnummer och samordningsnummer,
4. 4 kap. 1 § om användningsbegränsningar för arkiverade personuppgifter,
5. 5 kap. 1 § första stycket och 5 kap. 2 § om begränsningar av vissa rättigheter och skyldigheter,
6. 6 kap. 1–5 §§ om tillsynsmyndighetens handläggning och beslut,
7. 7 kap. 1, 3 och 4 §§ om administrativa sanktionsavgifter,

<sup>1</sup> Ändringen innebär bl.a. att andra och tredje stycket tas bort.

12. 48 § om skadestånd, och 8. 8 kap. 1 § om skadestånd,  
 13. 51 § första stycket, 52 § och  
 första stycket och 53 § om 9. 8 kap. 2–4 och 6 §§ om  
 överklagande. överklagande.

*Om personuppgifter ska gallras enligt denna lag, eller enligt föreskrifter som har meddelats i anslutning till lagen, gäller inte 8 § andra stycket personuppgiftslagen.*

*Förbud enligt 44 eller 45 § personuppgiftslagen får inte förenas med vite.*

### 13 §

Personuppgifter som behandlas enligt 11 och 12 §§ får även behandlas när det är nödvändigt för att tillhandahålla information till

1. riksdagen eller regeringen,
2. en annan myndighet eller en enskild, om uppgifterna lämnas med stöd av lag eller förordning, eller
3. en utländsk myndighet, ett EU-organ eller en mellanfolklig organisation, om utlämnandet av uppgifterna följer av Sveriges medlemskap i Europeiska unionen eller av uppgiftsskyldighet enligt en internationell konvention som Sverige har tillträtt eller enligt ett av riksdagen godkänt avtal med främmande stat eller mellanfolklig organisation.

I ett enskilt fall får personuppgifter som behandlas enligt 11 och 12 §§ även behandlas för att tillhandahålla information för något annat ändamål än de som anges i första stycket under förutsättning att *ändamålet inte är oförenligt med det ändamål som uppgifterna samlades in för.*

I ett enskilt fall får personuppgifter som behandlas enligt 11 och 12 §§ även behandlas för att tillhandahålla information för något annat ändamål än de som anges i första stycket under förutsättning att *behandlingen är tillåten enligt artiklarna 5.1 b och 6.4 i Europaparlamentets och rådets förordning (EU) 2016/679.*



## 13 a §

*Personuppgifter som behandlas eller har behandlats enligt 11–12 §§ får även behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 i Europaparlamentets och rådets förordning (EU) 2016/679.*

*Första stycket gäller inte om personuppgifter ska gallras enligt denna lag, eller enligt föreskrifter som har meddelats i anslutning till lagen.*

## 15 §

*Sådana känsliga personuppgifter som anges i 13 § personuppgiftslagen (1998:204) får endast behandlas*

*Sådana särskilda kategorier av uppgifter som anges i artikel 9.1 i Europaparlamentets och rådets förordning (EU) 2016/679 (känsliga personuppgifter) får endast behandlas*

1. för de ändamål som anges i 11 § 1–4 och 6 samt 13 § om uppgifterna är absolut nödvändiga för syftet med behandlingen, eller

2. i löpande text för det ändamål som anges i 12 § 2, om uppgifterna är absolut nödvändiga för att fullgöra arbetsuppgifter i sådan verksamhet som anges i 2 §.

*Vad som sägs i första stycket hindrar inte att känsliga personuppgifter behandlas med stöd av 15 a §.*

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela

1. ytterligare föreskrifter om inskränkningar av möjligheten att behandla känsliga personuppgifter, och
2. föreskrifter om gallring.

## 17 §

Vid sökning i personuppgifter är det förbjudet att *som sökbegrepp använda uppgifter som avslöjar*

1. *ras eller etniskt ursprung,*
2. *politiska åsikter,*
3. *religiös eller filosofisk övertygelse,*
4. *medlemskap i fackförening,*
5. *hälsa, eller*
6. *sexualliv.*

Vid sökning i personuppgifter är det förbjudet att *använda sökbegrepp som avslöjar känsliga personuppgifter enligt 15 §.*

*Vad som sägs i första stycket hindrar inte att känsliga personuppgifter behandlas med stöd av 15 a §.*

## 18 §

Vid behandling av personuppgifter för ändamål som anges i 12 § 2 får personuppgifter som direkt pekar ut den registrerade inte användas som sökbegrepp.

Vid sökning i personuppgifter får *sådana uppgifter om lagöverträdelser m.m. som anges i 21 § personuppgiftslagen (1998:204)* inte användas som sökbegrepp. Uppgifter om beslut om förvar enligt utlänningslagen (2005:716) får dock användas som sökbegrepp.

Vid sökning i personuppgifter får *uppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden* inte användas som sökbegrepp. Uppgifter om beslut om förvar enligt utlänningslagen (2005:716) får dock användas som sökbegrepp.

***Begränsningar av vissa rättigheter och skyldigheter***

## 18 a §

*Bestämmelserna om den registrerades rätt att få information om en person-*

*uppgiftsincident enligt artikel 34 i Europaparlamentets och rådets förordning (EU) 2016/679, gäller inte om den personuppgiftsansvarige, enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning, inte får lämna ut uppgifter till den registrerade.*

## 20 §

Polismyndigheten har rätt att ta del av personuppgifter som Migrationsverket behandlar enligt 11 eller 14 § vid direktåtkomst enligt 19 §. Säkerhetspolisen och utlandsmyndigheterna har motsvarande rätt att vid direktåtkomst ta del av uppgifter som Migrationsverket behandlar enligt 11 §.

Migrationsverket ska på begäran av Polismyndigheten, Säkerhetspolisen eller en utlandsmyndighet lämna ut personuppgifter som verket behandlar enligt 11 § 1 eller 2. Migrationsverket ska också på begäran av Polismyndigheten lämna ut personuppgifter som verket behandlar enligt 14 § andra stycket 1, 2 eller 5.

Om det finns skäl för det ska Migrationsverket på eget initiativ lämna uppgifter som avses i andra stycket andra meningen till Polismyndigheten.

Polismyndigheten har rätt att ta del av personuppgifter som Migrationsverket behandlar enligt 11 eller 15 a § vid direktåtkomst enligt 19 §. Säkerhetspolisen och utlandsmyndigheterna har motsvarande rätt att vid direktåtkomst ta del av uppgifter som Migrationsverket behandlar enligt 11 §.

Migrationsverket ska på begäran av Polismyndigheten, Säkerhetspolisen eller en utlandsmyndighet lämna ut personuppgifter som verket behandlar enligt 11 § 1 eller 2. Migrationsverket ska också på begäran av Polismyndigheten lämna ut personuppgifter som verket behandlar enligt 15 a § andra stycket 1, 2 eller 5.

## 21 §

*Trots hänvisningen till 33 § personuppgiftslagen (1998:204) i till tredjeland även utan den*

8 § första stycket 8 är det tillåtet att även utan den registrerades samtycke föra över personuppgifter till tredjeland om överföringen är absolut nödvändig för de ändamål som anges i 11 § 1 och 2 samt 12 § 1, såvida det inte möter hinder av sekretess enligt offentlighets- och sekretesslagen (2009:400).

*Sådan överföring får ske även om det inte finns något beslut om adekvat skyddsnivå enligt artikel 45.3 eller lämpliga skyddsåtgärder enligt artikel 46 i Europaparlamentets och rådets förordning (EU) 2016/679.*

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om begränsningar av möjligheten att föra över personuppgifter till tredjeland.

---

1. Denna lag träder i kraft den 1 maj 2018 i fråga om 3 och 3 a §§ och i övrigt den 25 maj 2018.

2. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats med stöd av de föreskrifterna.

## 1.2 Förslag till förordning om ändring i utlänningsdataförordningen (2016:30)

Härigenom föreskrivs att 9 § utlänningsdataförordningen (2016:30) ska ha följande lydelse.

*Nuvarande lydelse*

*Föreslagen lydelse*

9 §

Polismyndighetens direkt-  
åtkomst ska begränsas till de  
personuppgifter som  
myndigheten behöver för de  
ändamål som anges i 11 § 1–4  
och 14 § andra stycket 2  
utlänningsdatalagen (2016:27).

Polismyndighetens direkt-  
åtkomst ska begränsas till de  
personuppgifter som  
myndigheten behöver för de  
ändamål som anges i 11 § 1–4  
och 15 a § andra stycket 2  
utlänningsdatalagen (2016:27).



## 2 Uppdraget och dess genomförande

### 2.1 Uppdraget

Mitt uppdrag är att lämna förslag på de författningsändringar som behövs för att komplettera EU:s dataskyddsförordning<sup>1</sup> i utlänningsdatalagen (2016:27) och utlänningsdataförordningen (2016:30). Enligt uppdragsbeskrivningen ska jag belysa vilka konsekvenser de föreslagna ändringarna bedöms få. Om förslagen förväntas leda till kostnadsökningar för det allmänna, ska jag föreslå hur dessa ska finansieras.

### 2.2 Avgränsningar

Det ligger inte inom uppdraget att presentera en heltäckande redogörelse för dataskyddsförordningens bestämmelser eller för skillnaderna mellan det gamla och det nya regelverket för personuppgiftsbehandling. Eventuella behov av förändringar i utlänningsdatalagen som inte är en följd av dataskyddsförordningen kan på grund av den tidsmässiga aspekten inte heller hanteras inom ramen för vårt uppdrag.

Utredningen om 2016 års dataskyddsdirektiv (Ju 2016:06) har vidare i uppdrag att lämna förslag till de författningsförändringar som krävs för att genomföra Europaparlamentets och rådets direktiv (EU) 2016/680 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter

---

<sup>1</sup> Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för enskilda 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).

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. Inom den utredningens uppdrag ligger även att analysera och beskriva 2016 års dataskyddsdirektivs tillämpningsområde. Dessa frågor behandlas således inte i denna promemoria.

### **2.3 Uppdragets genomförande**

Utredningsarbetet har bedrivits på sedvanligt sätt, dock utan särskild expert- eller referensgrupp. I stället har samråd med Migrationsverket och Polismyndigheten skett kontinuerligt under utredningstiden. Vi har också samrått med Utredningen om 2016 års dataskyddsdirektiv och ingått i en informell samordningsgrupp med andra utredningar som haft i uppdrag att anpassa svensk rätt till EU:s dataskyddsreform.

### **2.4 Promemorians disposition**

Promemorian är indelad i 22 kapitel.

I kapitel 1 finns författningsförslaget. Kapitel 2 behandlar uppdraget och dess genomförande. I kapitel 3 redogör vi för gällande internationell och nationell rätt på personuppgiftsområdet.

EU:s dataskyddsreform behandlas i kapitel 4. Därefter följer en bedömning av möjligheten att behålla eller införa nationella registerförfattningar (kapitel 5) och av vilken eller vilka av dataskyddsförordningens s.k. rättsliga grunder som ger stöd för den personuppgiftsbehandling som utförs inom utlänningsdatalagens tillämpningsområde (kapitel 6). I kapitel 7 behandlar vi utlänningsdatalagens syfte och tillämpningsområde. Kapitel 8 innehåller en bedömning av lagens ändamålsbestämmelser och behovet av att komplettera dessa. Sedan följer i kapitel 9 våra överväganden av lagens förhållande till annan lagstiftning och hur dess befintliga hänvisningar till personuppgiftslagen (1998:204) ska hanteras. I kapitel 10 behandlar vi personuppgiftsansvaret och i kapitel 11 bestämmelsen om personuppgiftsombud.

Vår bedömning av hur dataskyddsförordningens bestämmelser om behandling av känsliga personuppgifter påverkar utlännings-



datalagen finns i kapitel 12. Kapitel 13 innehåller våra överväganden vad gäller tillgången till personuppgifter. Därefter redogör vi, i kapitel 14, för de viktigaste förändringarna dataskyddsförordningen innebär för de registrerades rättigheter. Där gör vi också en analys av möjligheterna och behovet av att begränsa de registrerades rättigheter i vissa fall. Därefter följer en bedömning av lagens bestämmelser om direktåtkomst och uppgiftsskyldighet (kapitel 15).

Våra överväganden vad gäller utlänningsdatalagens och utlänningsdataförordningens bestämmelser om tredjelandsöverföringar av personuppgifter finns i kapitel 16. I kapitel 17 behandlas vilka förändringar som krävs för att bevarande av personuppgifter fortsatt ska vara tillåtet inom utlänningsdatalagens tillämpningsområde. Kapitlet innehåller också vår bedömning vad gäller lagens bestämmelser om avskiljande och gallring. Föreskriftsrätten behandlas i kapitel 18, förändringar av överklagandebestämmelser i kapitel 19 och frågor om övergångs- och ikraftträdandebestämmelser i kapitel 20. Slutligen behandlas konsekvenserna av våra förslag i kapitel 21. I kapitel 22 finns en kortfattad författningskommentar till de författningsändringar som föreslås.

För att läsaren ska få en bättre överblick över hur våra förslag påverkar utlänningsdatalagens innehåll finns i *bilaga 2* en sammanställning av hur den lagen kommer att se ut i sin helhet om våra förslag genomförs (konsoliderad version). Dataskyddsförordningen finns bifogad som *bilaga 3*.



## 3 Gällande rätt

### 3.1 FN

Förenta Nationerna (FN) antog år 1948 den allmänna förklaringen om de mänskliga rättigheterna, som inte är formellt bindande för medlemsstaterna. Vidare har det inom FN utarbetats en internationell konvention om medborgerliga och politiska rättigheter, som trädde i kraft 1976. Sverige har anslutit sig till konventionen. I både den allmänna förklaringen och konventionen (artikel 12 respektive artikel 17) finns bestämmelser om rätten till skydd för enskildas privata sfär. Av artikel 29 i den allmänna förklaringen framgår vidare att en person vid utövandet av sina rättigheter och friheter 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.

FN:s generalförsamling antog år 1990 riktlinjer om datoriserade register med personuppgifter, som innehåller de grundläggande principer som medlemsstaterna ska ta hänsyn till vid lagstiftning avseende sådana register.

### 3.2 OECD

OECD:s (Organisationen för ekonomiskt samarbete och utveckling) råd antog år 1980 riktlinjer i fråga om integritetsskyddet och personuppgiftsflödet över gränserna. Samtidigt utfärdades en rekommendation till medlemsländernas regeringar om att beakta riktlinjerna i nationell lagstiftning. Riktlinjerna gäller för både privat och offentlig sektor, de ska uppfattas som minimiregler och de motsvarar i princip de bestämmelser som finns

i Europarådets dataskyddskonvention. Samtliga medlemsländer har åtagit sig att följa riktlinjerna.

### **3.3 Europarådet**

#### **3.3.1 Europakonventionen**

Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) gäller som lag i Sverige.<sup>1</sup> Av 2 kap. 19 § regeringsformen framgår också 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 skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens. Offentliga myndigheter får inte inskränka denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till den nationella säkerheten, den allmänna säkerheten, landets ekonomiska välbefinnande, förebyggande av oordning eller brott, till skydd för hälsa eller moral eller till skydd för andra personers fri- och rättigheter.

#### **3.3.2 Dataskyddskonventionen**

Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (dataskyddskonventionen) trädde i kraft år 1985. Samtliga EU:s medlemsstater har ratificerat konventionen, som är bindande.

Konventionen innehåller grundläggande principer för dataskydd som de konventionsanslutna staterna ska beakta i sin nationella lagstiftning. Syftet med konventionen är att säkerställa rätten till personlig integritet i samband med automatiserad behandling av personuppgifter. 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 data-

---

<sup>1</sup> Lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.

behandling 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.

Utöver dataskyddskonventionen har det inom Europarådet utarbetats flera icke bindande rekommendationer på dataskyddsområdet.

## 3.4 EU

### 3.4.1 Stadgan

Europeiska unionens stadga om de grundläggande rättigheterna (stadgan) är en del av EU:s primärrätt och bindande för både EU:s institutioner och medlemsstaterna vid tillämpning av unionsrätten.<sup>2</sup>

Enligt artikel 7 i stadgan har var och en rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Av artikel 8 i stadgan framgår att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Det framgår också att personuppgifter 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 också 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. Enligt artikel 47 i stadgan har var och en vars unionsrättsligt garanterade fri- och rättigheter har kränkts rätt till ett effektivt rättsmedel inför en domstol.

### 3.4.2 Dataskyddsdirektivet och dataskyddsrambeslutet

Den allmänna regleringen om behandling av personuppgifter inom EU finns för närvarande 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. Vi kommer fortsatt i denna promemoria att hänvisa till detta direktiv som *1995 års dataskyddsdirektiv*.

---

<sup>2</sup> Se artikel 61.1 i Lissabonfördraget och artikel 51 i stadgan.

Direktivets syfte är, enligt artikel 1.1, att garantera att medlemsstaterna skyddar fysiska personers grundläggande fri- och rättigheter, särskilt rätten till privatliv, i samband med behandling av personuppgifter. Av artikel 1.2 framgår vidare att syftet är att främja ett fritt flöde av personuppgifter mellan medlemsstaterna i EU.

Behandling av personuppgifter på områden som faller eller tidigare föll utanför unionsrätten, till exempel allmän säkerhet och försvar samt statens verksamhet på straffrättens område, omfattas inte av 1995 års dataskyddsdirektiv. 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, enligt artikel 1.2 i beslutet, tillämpligt på personuppgiftsbehandling i form av överföring mellan medlemsstaterna i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder. Dataskyddsrambeslutet gäller dock inte för nationell personuppgiftsbehandling. Från tillämpningsområdet undantas också personuppgiftsbehandling inom området nationell säkerhet. Dataskyddsrambeslutet har genomförts i svensk rätt främst genom lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen.

## **3.5 Svensk rätt**

### **3.5.1 Regeringsformen**

Enligt 2 kap. 6 § andra stycket regeringsformen är var och en gentemot det allmänna 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 §§ RF 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.

### 3.5.2 Personuppgiftslagen

Sverige har genomfört 1995 års dataskyddsdirektiv främst genom personuppgiftslagen (1998:204), förkortad PuL. Lagen trädde i kraft den 24 oktober 1998 och har till syfte att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Lagen följer i princip samma struktur som 1995 års dataskyddsdirektiv och innehåller – liksom direktivet – bestämmelser om bland annat personuppgiftsansvar, grundläggande krav för behandling av personuppgifter och information till den registrerade. Personuppgiftslagen gäller för både myndigheter och enskilda som behandlar personuppgifter. Lagen är subsidiär, vilket innebär att dess bestämmelser inte ska tillämpas om det finns avvikande bestämmelser i en annan lag eller förordning. Det finns en stor mängd sådana bestämmelser i de sektorsspecifika s.k. registerförfattningar (eller informationshanteringsförfattningar<sup>3</sup>) som reglerar myndigheternas personuppgiftsbehandling.

Personuppgiftslagen kompletteras av bestämmelser i personuppgiftsförordningen (1998:1191), 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.

### 3.6 Registerförfattningar för utlännings- och medborgarskapslagstiftningen

För myndigheters behandling av personuppgifter finns, som vi nyss nämnt, en stor mängd särskilda registerförfattningar. Syftet med dessa författningar är att anpassa personuppgiftsregleringen till de särskilda behov som myndigheterna har i sina respektive verksamheter samt att göra avvägningar mellan verksamhetens

---

<sup>3</sup> Jfr Informationshanteringsutredningens betänkande (SOU 2015:39 s. 967 ff.).

behov av effektivitet och den enskildes rätt till skydd för sin integritet.

Migrationsverkets, utlandsmyndigheternas, Polismyndighetens och Säkerhetspolisens personuppgiftsbehandling i verksamhet enligt utlännings- och medborgarskapslagstiftningen reglerades tidigare av förordningen (2001:720) om behandling av personuppgifter i verksamhet enligt utlännings- och medborgarskapslagstiftningen, som trädde i kraft den 1 oktober 2001.

Personuppgiftsbehandlingen på utlännings- och medborgarskapsområdet sker till stora delar utan att den enskildes samtycke inhämtas. De personuppgifter som behandlades enligt den tidigare förordningen om behandling av personuppgifter i verksamhet enligt utlännings- och medborgarskapslagstiftningen omfattade vidare en mängd uppgifter om ett stort antal personer som – även om detta inte var syftet med behandlingen – kunde anses innebära övervakning eller kartläggning av den enskildes personliga förhållanden. Mot den bakgrunden ansåg regeringen att personuppgiftsbehandlingen på utlännings- och medborgarskapsområdet åtminstone delvis innebär betydande intrång i den personliga integriteten och därmed faller inom det område som enligt 2 kap. 6 och 20 §§ RF måste regleras i lag (se avsnitt 3.5.1).

En översyn av regelverket resulterade i utlänningsdatalagen (2016:27) och utlänningsdataförordningen (2016:30), vilka trädde i kraft den 12 februari 2016. Utlänningsdatalagen med den tillhörande förordningen gäller vid behandling av personuppgifter i vissa angivna verksamheter enligt utlännings- och medborgarskapslagstiftningen hos Migrationsverket, utlandsmyndigheterna och Polismyndigheten. De gäller även i vissa fall när personuppgifter i dessa verksamheter vidarebehandlas för att lämnas ut till exempelvis riksdagen, regeringen eller till en annan myndighet eller en enskild med stöd av lag eller förordning. Utlänningsdatalagen gäller i stället för personuppgiftslagen, men innehåller hänvisningar till de bestämmelser i den lagen som ska gälla inom tillämpningsområdet. Regelverket är tänkt att vara flexibelt för att passa de olika myndigheternas verksamhet och för att möjliggöra utveckling och effektivisering av myndigheternas verksamhet och it-stöd. På grund av den snabba tekniska utvecklingen har målsättningen också



varit att i så stor utsträckning som möjligt göra utlänningsdatalagen och utlänningsdataförordningen teknikneutrala.<sup>4</sup>

---

<sup>4</sup> Se förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 37).



## 4 Nya regelverk för personuppgiftsbehandling

### 4.1 EU:s dataskyddsreform

Europeiska kommissionen presenterade den 25 januari 2012 förslag till en genomgripande reform av EU:s regler om skydd för personuppgifter. Reformen omfattar dels en förordning som ersätter 1995 års dataskyddsdirektiv<sup>1</sup> och dels ett nytt direktiv med särregler för personuppgiftsbehandling i främst den brottsbekämpande sektorn.

#### 4.1.1 Dataskyddsförordningen

Den 27 april 2016 antogs Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för enskilda 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). Den vedertagna förkortningen för förordningen är GDPR. I likhet med de flesta andra utredningar som nu ser eller har sett över svensk lagstiftning på detta område har vi dock valt att i vår promemoria som kortform för den nya rättsakten använda oss av *dataskyddsförordningen*.

Av skäl 13 till dataskyddsförordningen framgår att syftet med förordningen bl.a. är att säkerställa en enhetlig skyddsnivå över hela unionen och att undvika avvikelser som hindrar den fria rörligheten av personuppgifter inom den inre marknaden.

---

<sup>1</sup> 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 kommer från och med den 25 maj 2018 att ersätta 1995 års dataskyddsdirektiv och utgöra grunden för generell personuppgiftsbehandling inom EU. Enligt artikel 288 andra stycket i Fördraget om Europeiska unionens funktionssätt ska en EU-förordning ha allmän giltighet och vara till alla delar bindande och direkt tillämplig i varje medlemsstat. Förordningens bestämmelser ska således tillämpas av enskilda, myndigheter och domstolar på samma sätt som om de vore nationella författningsbestämmelser. Även om dataskyddsförordningen är direkt tillämplig innehåller den många bestämmelser som förutsätter eller ger utrymme för kompletterande nationella bestämmelser av olika slag.

#### 4.1.2 2016 års dataskyddsdirektiv

Samtidigt med dataskyddsförordningen antogs 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. I fortsättningen kommer vi i vår promemoria att kalla detta direktiv för *2016 års dataskyddsdirektiv*. Direktivet ska vara genomfört i nationell rätt senast den 6 maj 2018.

Enligt artikel 1.1 i 2016 års dataskyddsdirektiv innehåller direktivet bestämmelser om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder. Även sådan personuppgiftsbehandling som utförs hos behöriga myndigheter för att skydda mot, förebygga och förhindra hot mot den allmänna säkerheten ingår i tillämpningsområdet. Av artikel 1.2 i direktivet framgår att syftet med direktivet är att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Det framgår också att syftet är att säkerställa att det utbyte av personuppgifter som krävs inom unionen mellan behöriga myndigheter varken begränsas eller förbjuds av skäl som

rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter.

Av artikel 2.1.d i dataskyddsförordningen jämförd med artikel 1.1 i 2016 års dataskyddsdirektiv framgår att förordningen inte gäller för sådan personuppgiftsbehandling som omfattas av direktivets tillämpningsområde.

## 4.2 Två nya svenska regelverk för personuppgiftsbehandling

När dataskyddsförordningen börjar tillämpas ska personuppgiftslagen upphävas.<sup>2</sup> Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) lämnat förslag till en ny lag; lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (förkortad dataskyddslagen). Som framgår av namnet ska denna lag komplettera EU:s dataskyddsförordning på ett generellt plan i svensk rätt. Dataskyddsutredningen har även lämnat förslag till en förordning till dataskyddslagen, förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning. I likhet med vad som gäller för personuppgiftslagen ska avvikande bestämmelser i annan lag eller förordning ha företräde framför bestämmelserna i dataskyddslagen.

Utöver denna generella reglering kommer kompletteringar till bestämmelserna i EU:s dataskyddsförordning att finnas i de sektorsspecifika registerförfattningar som i stor utsträckning reglerar svenska myndigheters personuppgiftsbehandling. Ett omfattande arbete pågår eller har nyligen pågått inom utredningsväsendet för att, i likhet med det uppdrag vi har fått, anpassa dessa sektorsspecifika författningar till det nya regelverket.

Den personuppgiftsbehandling som sker hos behöriga myndigheter i syfte att bl.a. förebygga, förhindra, utreda, avslöja eller lagföra brott samt verkställa straffrättsliga påföljder kommer dock att styras av 2016 års dataskyddsdirektiv. Utredningen om 2016 års dataskyddsdirektiv har i sitt delbetänkande (SOU 2017:29) föreslagit att detta direktiv ska genomföras i svensk rätt

---

<sup>2</sup> Se kommittédirektiv till Dataskyddsutredningen (Dir. 2016:15 s. 6).

genom en ny generellt tillämplig lag, kallad brottsdatalagen. Denna lag ska enligt utredningens förslag kompletteras av en förordning, kallad brottsdataförordningen.

Även inom brottsdatalagens tillämpningsområde finns det en mängd sektorsspecifika registerförfattningar. Det ligger inom Utredningen om 2016 års dataskyddsdirektivs uppdrag att analysera och bedöma i vilken utsträckning dessa registerförfattningar behöver förändras med hänsyn till 2016 års dataskyddsdirektivs förpliktelser och till den nya ramlagstiftning som brottsdatalagen kommer att utgöra.<sup>3</sup>

För många myndigheter – t.ex. Polismyndigheten och domstolarna – får EU:s dataskyddsreform effekten att personuppgiftsbehandlingen i vissa delar av verksamheten tillhör dataskyddsförordningens tillämpningsområde medan den i andra delar av verksamheten tillhör 2016 års dataskyddsdirektivs tillämpningsområde. Det avgörande för vilket av regelverken som är tillämpligt för en myndighets personuppgiftsbehandling kommer att vara dels syftet med behandlingen, dels vilken typ av myndighet som utför behandlingen. Mycket kort kan sägas att om syftet med behandlingen är att förebygga, förhindra, utreda, avslöja eller lagföra brott, att verkställa straffrättsliga påföljder eller att skydda mot, förebygga eller förhindra hot mot den allmänna säkerheten, kommer behandlingen att omfattas av brottsdatalagen och de särskilda registerförfattningar som finns inom dess tillämpningsområde. En förutsättning för detta är dock att behandlingen utförs av en sådan myndighet som är behörig enligt brottsdatalagen. All övrig personuppgiftsbehandling kommer att regleras av dataskyddsförordningen, den svenska dataskyddslagen och de särskilda registerförfattningar som kompletterar detta regelverk.

Som vi nämnt ovan (avsnitt 4.1.2) är det i denna del tillämpningsområdet för 2016 års dataskyddsdirektiv som avgör när dataskyddsförordningen ska tillämpas. Ledning för hur myndigheterna ska bedöma frågan om vilket regelverk som kommer att bli tillämpligt kan lämpligen hämtas ur Utredningen om 2016 års dataskyddsdirektivs delbetänkande (SOU 2017:29, kap. 7 och 8). Här finns en omfattande analys av brottsdatalagens

---

<sup>3</sup> Se kommittédirektiv till Utredningen om 2016 års dataskyddsdirektiv (Dir. 2016:21 s. 9).

tillämpningsområde och de gränsdragningsfrågor som kan uppstå vid myndigheters personuppgiftsbehandling.





## 5 Nationella registerförfattningar

### 5.1 Registerförfattningarnas förenlighet med dataskyddsförordningen

När dataskyddsförordningen börjar tillämpas kommer den att vara direkt tillämplig på all personuppgiftsbehandling som i medlemsstaterna utförs inom dess materiella och territoriella tillämpningsområde. Personuppgiftslagen kommer då att upphävas.<sup>1</sup> Som vi nämnt i avsnitt 4.2 har Dataskyddsutredningen dock i sitt betänkande (SOU 2017:39) föreslagit att den nya dataskyddslagen ska komplettera dataskyddsförordningen i svensk rätt. Dataskyddslagen föreslås, i likhet med personuppgiftslagen, vara subsidiär i förhållande till bestämmelser om behandling av personuppgifter i andra författningar.

När det gäller personuppgiftsbehandling som är nödvändig för att fullgöra en rättslig förpliktelse, som ett led i myndighetsutövning eller för att utföra en uppgift av allmänt intresse (se avsnitt 6.3) ger artikel 6.2 i dataskyddsförordningen medlemsstaterna möjlighet att behålla eller införa mer specifika bestämmelser, där bl.a. specifika krav för uppgiftsbehandlingen och andra åtgärder för att säkerställa en laglig och rättvis behandling närmare fastställs. Av skäl 10 till dataskyddsförordningen framgår vidare att möjligheten att specificera bestämmelserna för personuppgiftsbehandling också gäller känsliga personuppgifter.

Även artikel 6.3 andra stycket i dataskyddsförordningen ger medlemsstaterna möjlighet att specificera villkoren för personuppgiftsbehandling. Här anges att den rättsliga grunden kan innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen. Som exempel nämns de allmänna

---

<sup>1</sup> Se kommittédirektiv till Dataskyddsutredningen (Dir 2016:15 s. 6).

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. Även förfaranden för behandling nämns. Här ingår åtgärder för att tillförsäkra en laglig och rättvis behandling, t.ex. i de särskilda situationer som framgår av nionde kapitlet. Det kapitlet reglerar bl.a. förhållandet till yttrande- och informationsfriheten samt offentlighetsprincipen. Även medlemsstaternas rätt att närmare bestämma på vilka villkor nationella identifikationsnummer får behandlas framgår av detta kapitel. Det anges också i artikel 6.3 att unionsrätten eller medlemsstaternas nationella rätt ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas. Av artikel 4.7 i dataskyddsförordningen framgår att vem som är personuppgiftsansvarig kan föreskrivas i den nationella rätten, om ändamålen och medlen för behandling fastställs av medlemstatens nationella rätt.

I artikel 6.3 andra stycket i dataskyddsförordningen anges förvisso att de särskilda bestämmelserna ska vara en del av "den rättsliga grunden". Dataskyddsutredningen (SOU 2017:39 s. 135) har vad gäller artikel 6 tolkat dataskyddsförordningen på så sätt att med den rättsliga grunden för personuppgiftsbehandling avses någon av de grunder för behandling som anges i artikel 6.1 (se kapitel 6). Den rättsliga grunden skulle med detta synsätt vara exempelvis den bestämmelse i nationell rätt där en myndighets uppgift av allmänt intresse eller dess myndighetsutövande uppdrag fastställs. I svensk rätt är det dock vanligare att denna "rättsliga grund" inte innehåller bestämmelser om personuppgiftsbehandling. I stället återfinns dessa bestämmelser ofta i sektorsspecifika registerförfattningar. Vi anser att det måste vara möjligt att tolka dataskyddsförordningen så att den ger handlingsutrymme att följa de nationella lagstiftningstraditionerna på området. Exemplifieringen av frågor som enligt artikel 6.3 andra stycket kan fastställas i den nationella rätten måste därmed för svensk del kunna ses som en exemplifiering av de bestämmelser som kan förekomma i registerförfattningarna.

## 5.2 Allmänna principer för behandling av personuppgifter

Dataskyddsutredningen gör i sitt betänkande (SOU 2017:39 s. 105) bedömningen att de svenska registerförfattningarna framför allt kommer att innehålla en precisering av de allmänna principer för personuppgiftsbehandling som framgår av artikel 5 i dataskyddsförordningen. Dessa principer motsvaras i stort av artikel 6 i 1995 års dataskyddsdirektiv, som införts i svensk rätt genom 9 § PuL. Artikel 5.1 i dataskyddsförordningen lyder i sin helhet som följer.

### Artikel 5

1. Vid behandling av personuppgifter ska följande gälla:

a) Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (*laglighet, korrekthet och öppenhet*).

b) 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*).

c) De ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (*uppgiftsminimering*).

d) 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*).

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, förstöring eller skada genom olycks-händelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (*integritet och konfidentialitet*).

Det är således dessa ovan angivna principer som registerförfattningarna till stor del är menade att precisera.

### 5.3 Bedömning

**Bedömning:** Dataskyddsförordningen hindrar inte den typ av nationell registerlagstiftning som utlänningsdatalagen utgör.

Dataskyddsförordningen hindrar inte heller att medlemsstaterna i registerförfattning inför mer restriktiva bestämmelser för myndigheternas personuppgiftsbehandling än vad som följer av förordningen eller utökar de nationella myndigheternas skyldigheter gentemot de registrerade.

Sammanfattningsvis anser vi att artikel 6.2 och 6.3 i dataskyddsförordningen ger medlemsstaterna möjlighet att i den nationella lagstiftningen närmare precisera hur personuppgifter får behandlas när behandlingen är nödvändig för att fullgöra en rättslig förpliktelse, som ett led i den personuppgiftsansvariges myndighetsutövning eller för att utföra en uppgift av allmänt intresse. Detta kan ske genom exempelvis den typ av registerlagstiftning som utlänningsdatalagen utgör. Medlemsstaterna har här enligt vår mening frihet att välja vilket område eller vilken verksamhet en registerförfattning ska reglera, så länge lagstiftningen omfattar sådant som ryms inom begreppen rättslig förpliktelse, uppgift av allmänt intresse eller myndighetsutövning.

Dataskyddsutredningen gör i sitt betänkande (SOU 2017:39 s. 105) bedömningen att registerförfattningarna framför allt kommer att innehålla en precisering av de allmänna principer för personuppgiftsbehandling som framgår av artikel 5 i dataskyddsförordningen. Det kan vidare nämnas att det är tillåtet för en medlemsstat, som genomför förtydliganden och begränsningar av dataskyddsförordningens bestämmelser genom den nationella rätten, att införliva delar av förordningen i nationell rätt. Detta

framgår av skäl 8 till dataskyddsförordningen. Ett direkt återgivande av de bestämmelser som finns i dataskyddsförordningen och som förvisso skulle ha gällt även utan ett sådant återgivande är därmed tillåtet i nationell rätt. Enligt skäl 8 kan syftet med detta bl.a. vara att göra de nationella bestämmelserna begripliga.

Dataskyddsförordningen innehåller inte något förbud mot att de personuppgiftsansvariga utökar skyddet för de personuppgifter som behandlas, går utöver sina skyldigheter vad gäller information till de registrerade eller liknande. Dataskyddsförordningen ger också, som framgår ovan, möjlighet till nationell specificering vad gäller myndigheternas behandling av personuppgifter. I artikel 1.2 i dataskyddsförordningen fastställs vidare att syftet med förordningen är att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd för personuppgifter. Mot den bakgrunden bedömer vi att nationell lagstiftning som skapar ett förstärkt skydd för sådana personuppgifter bör vara förenlig med dataskyddsförordningen. Medlemsstaterna bör således ha möjlighet att införa mer restriktiva bestämmelser för sina myndigheters personuppgiftsbehandling än vad som följer av dataskyddsförordningen. Det bör även vara möjligt för medlemsstaterna att utöka de nationella myndigheternas skyldigheter gentemot de registrerade.



## 6 Rättslig grund för personuppgiftsbehandlingen inom tillämpningsområdet

Dataskyddsförordningen utgår, liksom 1995 års dataskyddsdirektiv, från att varje behandling av personuppgifter måste vila på en rättslig grund. Enligt artikel 6.1 i dataskyddsförordningen får personuppgifter endast behandlas om någon av de rättsliga grunder som räknas upp i artikeln föreligger. De rättsliga grunder som närmast kommer i fråga för den personuppgiftsbehandling som utförs i Migrationsverkets, utlandsmyndigheternas och Polismyndighetens verksamhet enligt utlännings- och medborgarskapslagstiftningen är enligt vår mening de som framgår av artikel 6.1 e i dataskyddsförordningen. Enligt denna bestämmelse är personuppgiftsbehandling tillåten om den är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Personuppgiftsbehandling är även tillåten om den är nödvändig för att fullgöra en rättslig förpliktelse som åligger den personuppgiftsansvarige. Detta framgår av artikel 6.1 c i dataskyddsförordningen.

Bestämmelserna i artikel 6.1 i dataskyddsförordningen motsvarar i stora drag artikel 7 i 1995 års dataskyddsdirektiv, som har genomförts i svensk rätt genom 10 § PuL. Enligt den sistnämnda bestämmelsen får personuppgifter behandlas även utan den registrerades samtycke om behandlingen är nödvändig bl.a. för att den personuppgiftsansvarige ska kunna fullgöra en rättslig skyldighet (punkten b), för att en arbetsuppgift av allmänt intresse ska kunna utföras (punkten d) eller för att den personuppgiftsansvarige ska kunna utföra en arbetsuppgift i samband med myndighetsutövning (punkten e).

Utöver att någon av de rättsliga grunderna i artikel 6.1 i dataskyddsförordningen måste finnas för att personuppgiftsbehandlingen ska vara laglig, finns i artikel 6.3 första stycket i förordningen ett uttryckligt krav på att grunden för personuppgiftsbehandlingen – dvs. den rättsliga förpliktelsen, myndighetsutövningen eller uppgiften av allmänt intresse – ska vara fastställd i enlighet med unionsrätten eller den nationella rätten.

Som framgår av ordalydelsen i artikel 6.1 c och e i dataskyddsförordningen innehåller dessa rättsliga grunder även ett nödvändighetsrekvisit. För att en myndighets personuppgiftsbehandling ska vara tillåten enligt artikel 6.1 e måste den vara *nödvändig* för att myndigheten ska kunna utföra den uppgift av allmänt intresse som den genom författning har tilldelats, alternativt *nödvändig* för att myndigheten ska kunna utföra den myndighetsutövning som den har anförtrotts. På samma sätt är en personuppgiftsbehandling laglig enligt artikel 6.1 c om den är *nödvändig* för att fullgöra en rättslig förpliktelse.

Dataskyddsutredningen konstaterar i sitt betänkande (SOU 2017:39 s. 105 f.) att det unionsrättsliga begreppet *nödvändig* inte har samma strikta innebörd som i svenska språket. Även om exempelvis en uppgift av allmänt intresse skulle kunna utföras utan behandling av personuppgifter, kan behandlingen ur ett unionsrättsligt perspektiv anses vara nödvändig och därmed tillåten enligt artikel 6 om den leder till effektivitetsvinster.<sup>1</sup>

Alla myndigheter utför en rad administrativa uppgifter som krävs för att myndigheten ska fungera, men som varken direkt eller indirekt kan sägas framgå av uppdraget. Dataskyddsutredningen konstaterar i sitt betänkande (a.a. s. 129) att en myndighet inte kan utföra sina fastställda uppgifter om den inte fungerar och att således även administrativa åtgärder som är nödvändiga för myndighetens förvaltning och funktion därmed är rättsligt grundade i dataskyddsförordningens mening.

Utöver att personuppgiftsbehandlingen ska vara nödvändig för den rättsliga förpliktelsen, utförandet av uppgiften av allmänt intresse eller myndighetsutövningen, måste behandlingen

---

<sup>1</sup> Se SOU 1997:39 s. 359, Dom Huber mot Tyskland, C-524/06, EU:C:2008:724 och dom Pharmacontiente mot Saúde e Higiene m.fl., C-683/13, EU:C:2014:2028.



naturligtvis även utföras i enlighet med de allmänna principer som framgår av artikel 5 i dataskyddsförordningen. Detta innebär bland annat att behandlingen måste vara skälig eller rimlig (*korrekthet*) i förhållande till den registrerade. Behovet av den konkreta behandlingen måste därmed alltid vägas emot den registrerades intresse av personlig integritet.

## 6.1 Dataskyddslagen

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) föreslagit att det i dataskyddslagen ska tas in en bestämmelse som tydliggör att begreppet *uppgift av allmänt intresse* avser 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. Dataskyddsutredningen har även föreslagit att dataskyddslagen ska innehålla en bestämmelse som tydliggör att myndighetsutövning utgör en rättslig grund för behandling av personuppgifter endast om den sker enligt lag eller annan författning.

Vidare föreslår Dataskyddsutredningen att dataskyddslagen ska innehålla en bestämmelse som tydliggör att en rättslig förpliktelse utgör en rättslig grund för behandling av personuppgifter endast om förpliktelsen gäller enligt lag eller annan författning, följer av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning.

De nyss nämnda bestämmelserna ska, enligt Dataskyddsutredningens förslag, finnas i 2 kap. 3 och 4 §§ dataskyddslagen. Dataskyddsutredningen framhåller i sitt betänkande (SOU 2017:39 s. 112) att den rättsliga grunden inte nödvändigtvis måste fastställas i eller i enlighet med en av riksdagen beslutad lag, men att den däremot måste vara fastställd i laga ordning, på ett konstitutionellt korrekt sätt. Detta bör enligt vår mening innebära att även exempelvis förordningar som meddelats av regeringen, med stöd av den restkompetens som följer av regeringsformen, kan utgöra den rättsliga grunden för personuppgiftsbehandling. Detsamma bör gälla befogenheter som anges i annan föreskrift än lag eller förordning, förutsatt att föreskriften har meddelats i den ordning

som följer av regeringsformens bestämmelser om normgivningskompetens.

## **6.2 Myndighetsutövning, uppgift av allmänt intresse eller rättslig förpliktelse?**

Vi kommer i detta avsnitt att kort redogöra för de av dataskyddsförordningens rättsliga grunder för personuppgiftsbehandling som vi anser är relevanta för den behandling som omfattas av utlänningsdatalagen. I vår redogörelse utgår vi i allt väsentligt från den analys av begreppen som Dataskyddsutredningen har gjort. För den som har behov av en mer utförlig redogörelse hänvisar vi till Dataskyddsutredningens betänkande i denna del.<sup>2</sup>

### **6.2.1 Uppgift av allmänt intresse**

Som framgår av artikel 6.1 e och artikel 6.3 första stycket i dataskyddsförordningen samt 2 kap. 4 § förslaget till dataskyddslag, är personuppgiftsbehandling laglig om den är nödvändig för att den personuppgiftsansvarige ska kunna utföra en uppgift av allmänt intresse som följer av lag eller annan författning eller av beslut som har meddelats med stöd av lag eller annan författning.

Dataskyddsförordningen skiljer sig från 1995 års dataskyddsdirektiv på så sätt att en myndighet inte längre kommer att kunna grunda sin personuppgiftsbehandling på en intresseavvägning mellan myndighetens berättigade intresse och den registrerades intressen eller grundläggande rättigheter och friheter. Den bestämmelse i dataskyddsförordningen som reglerar personuppgiftsbehandling efter en sådan intresseavvägning, artikel 6.1 f, gäller nämligen inte för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter. Även myndigheternas utrymme för att grunda personuppgiftsbehandlingen på samtycke från den registrerade kan antas minska genom dataskyddsförordningen. I skäl 43 till förordningen anges att samtycke inte

---

<sup>2</sup> SOU 2017:39 kapitel 8.

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.

Dataskyddsutredningen anser att mycket talar för att begreppet uppgift av allmänt intresse har fått en vidare unionsrättslig betydelse genom dataskyddsförordningen än det hittills har haft i svensk rätt.<sup>3</sup> Dataskyddsutredningen gör vidare bedömningen att begreppet uppgift av allmänt intresse rent språkligt kan antas avse något som är av intresse för eller berör många människor på ett bredare plan. Av skäl 45 till dataskyddsförordningen följer också att allmänintresset inbegriper hälso- och sjukvårdsändamål, folkhälsa, socialt skydd och förvaltning av hälso- och sjukvårdstjänster. Dataskyddsutredningen gör vidare bedömningen att alla uppgifter som utförs av statliga myndigheter i syfte att uppfylla ett uttryckligt uppdrag av riksdag eller regering är av allmänt intresse.<sup>4</sup>

## 6.2.2 Myndighetsutövning

Enligt artikel 6.1 e och artikel 6.3 första stycket i dataskyddsförordningen samt 2 kap. 4 § förslaget till dataskyddslag, är personuppgiftsbehandling laglig om den är nödvändig som ett led i myndighetsutövning som den personuppgiftsansvarige utövar enligt lag eller annan författning.

Dataskyddsutredningen anser att man bör kunna utgå från att det som i Sverige brukar anses vara myndighetsutövning även faller under motsvarande unionsrättsliga begrepp.<sup>5</sup> Myndighetsutövning definieras i svensk rätt ofta som ”utövning av befogenhet att bestämma om förmån, rättighet, skyldighet, disciplinär bestraffning eller annat jämförbart förhållande”. Definitionen härstammar från 3 § i 1971 års förvaltningslag.<sup>6</sup>

---

<sup>3</sup> Se Dataskyddsutredningens betänkande (SOU 2017:39 s. 123).

<sup>4</sup> A.a. s. 124.

<sup>5</sup> A.a. s. 119, med hänvisning till Datalagskommitténs betänkande (SOU 1997:39 s. 365).

<sup>6</sup> Holmberg m.fl. Grundlagarna, Zeteo, kommentar till RF 12:4 och prop. 1971:30 s. 333

Begreppet myndighetsutövning förekommer också i bl.a. skadeståndsrättsliga regler. I förarbetena till 3 kap. 2 § skadeståndslagen (1972:207) anges att myndighetsutövning avser beslut eller åtgärder som är ett uttryck för det allmännas rätt att utöva makt över medborgarna. Karakteristiskt är att den enskilde står i ett beroendeförhållande till myndigheten, som bestämmer över den enskildes rättigheter och skyldigheter på ett sätt som inte förekommer i privaträttsliga sammanhang.<sup>7</sup>

Myndighetsutövningen är således ytterst ett uttryck för samhällets maktbefogenheter i förhållande till medborgarna. Befogenheten till myndighetsutövning måste vara grundad på lag eller annan författning eller på annat sätt kunna härledas ur bemyndiganden från de högsta statsorganen. Till myndighetsutövning hör först och främst sådan offentlig verksamhet, varigenom myndigheterna ensidigt bestämmer om enskildas skyldigheter eller om ingrepp i enskildas frihet eller egendom. Hit hör alltså beslut som innebär ålägganden att göra eller underlåta något eller som avser ingrepp i personlig frihet eller egendom, men även rent faktiska åtgärder som innebär sådana ingrepp, vare sig de grundas på formella beslut eller inte. Så långt kan begreppet myndighetsutövning sägas sammanfalla med begreppet offentlig maktutövning. Men även åtskilliga gynnande beslut faller in under begreppet myndighetsutövning, exempelvis beslut om sociala förmåner, statsbidrag och liknande. Den enskilde står här i ett beroendeförhållande till det allmänna, som ensamt har möjlighet att tillmötesgå hans eller hennes anspråk och därigenom i viss mening kan sägas utöva makt mot honom eller henne. Till myndighetsutövning bör vidare hänföras vissa beslut, vilka till skillnad från de hittills nämnda inte innehåller direkta handlingsmönster utan har indirekta rättsverkningar gentemot den enskilde, t.ex. registreringsbeslut och beslut om utfärdande av legitimationshandlingar samt beslut i samband med obligatorisk kontrollverksamhet.

Utanför begreppet myndighetsutövning faller råd, upplysningar och andra icke bindande uttalanden samt sådan faktisk verksamhet som inte innebär tvång mot den enskilde (t.ex. undervisning eller sjukvård). Till myndighetsutövning räknas inte heller sådan

---

<sup>7</sup> Jfr prop. 1972:5 s. 498 f. och t.ex. NJA 2013 s. 1210.

verksamhet som stat eller kommun utövar i privaträttsliga former. Gränsdragningen mellan offentligrättsliga och privaträttsliga regler är sålunda av stor vikt när det gäller att bestämma begreppet myndighetsutövning.<sup>8</sup>

### 6.2.3 Rättslig förpliktelse

Enligt artikel 6.1 c och artikel 6.3 första stycket i dataskyddsförordningen samt 2 kap. 3 § förslaget till dataskyddslag är personuppgiftsbehandling laglig om den är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som följer av lag eller annan författning eller av beslut som har meddelats med stöd av lag eller annan författning.

Dataskyddsutredningen gör bedömningen att det faktum att den rättsliga förpliktelsen måste ha en legal grund inte innebär 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.<sup>9</sup>

Dataskyddsutredningen konstaterar att även domstolar och statliga myndigheter vid sidan av sina uppgifter och uppdrag kan sägas ha rättsliga förpliktelser och att det inte finns något i artikel 6.1 c i dataskyddsförordningen som begränsar tillämpningen till den privata sektorn. Domstolar och myndigheter har också andra författningsreglerade förpliktelser som i sig kräver personuppgiftsbehandling, exempelvis när det gäller personaladministration.<sup>10</sup> Datainspektionen har vidare ansett att den skyldighet för myndigheter som följer av offentlighetsprincipen är en sådan rättslig skyldighet som avses i personuppgiftslagen och som motsvaras av dataskyddsförordningens begrepp rättslig förpliktelse.<sup>11</sup>

---

<sup>8</sup> Lundell/Strömberg, Allmän förvaltningsrätt, 26 uppl., s. 20–21.

<sup>9</sup> Se Dataskyddsutredningens betänkande (SOU 2017:39 s. 113 f).

<sup>10</sup> A.a. s. 116 f, jfr även SOU 1997:39 s. 363.

<sup>11</sup> Datainspektionens rapport 2005:3 Övervakning i arbetslivet – Kontroll av de anställda Internet och e-postanvändning m.m. s. 15.

## **6.3 Den rättsliga grunden finns i artikel 6.1 c och e i dataskyddsförordningen**

### **6.3.1 Myndigheternas uppdrag på utlännings- och medborgarskapsområdet**

Utlänningsdatalagen gäller för personuppgiftsbehandling i viss verksamhet som Migrationsverket, utlandsmyndigheterna och Polismyndigheten utför enligt utlännings- och medborgarskapslagstiftningen. Det närmare tillämpningsområdet framgår av 2–6 §§ utlänningsdatalagen och behandlas i kapitel 7. För att kunna ta ställning till vilken eller vilka av dataskyddsförordningens rättsliga grunder som utgör det rättsliga stödet för myndigheternas personuppgiftsbehandling inom utlännings- och medborgarskapsområdet finns det enligt vår mening emellertid behov av att översiktligt redogöra för de uppgifter myndigheterna utför inom detta område.

Migrationsverket är – enligt 1 § första stycket förordningen (2007:996) med instruktion för Migrationsverket – förvaltningsmyndighet för frågor som rör uppehållstillstånd, arbetstillstånd, visering, mottagande av asylsökande, anvisningar till kommuner av nyanlända, återvändande, medborgarskap och återvandring. Verket ska vidare, enligt bestämmelsens andra stycke, fullgöra de uppgifter som myndigheten har enligt utlännings- och medborgarskapslagstiftningen, lagstiftningen om mottagande av asylsökande m.fl., lagstiftningen om mottagande av vissa nyanlända invandrare för bosättning samt andra författningar.

Med utlandsmyndigheterna menas beskickningar, delegationer vid internationella organisationer och karriärkonsulat. Detta framgår av 1 kap. 2 § förordningen (2014:115) med instruktion för utrikesrepresentationen. Enligt 3 kap. 9 § samma förordning ska beskickningar och konsulat handlägga migrationsärenden enligt EU:s förordningar och enligt utlänningslagstiftningen. Av den sistnämnda bestämmelsen framgår också att beskickningar och konsulat ska biträda Migrationsverket, Polismyndigheten och Säkerhetspolisen i ärenden enligt utlänningslagstiftningen. Sådant biträde kan till exempel bestå i att hjälpa Migrationsverket att kontrollera att de uppgifter som en asylsökande har lämnat i sin ansökan är korrekta eller att kontrollera om en handling som en

utlänning återoppar är äkta.<sup>12</sup> Utlandsmyndigheterna ska vidare, enligt 2 kap. 15 § utlänningsförordningen (2006:97), ta emot ansökningar om främlingspass från utlänningar som inte befinner sig i Sverige. Av 4 kap. 20 § utlänningsförordningen följer att en ansökan om uppehållstillstånd ges in till och utreds av en svensk beskickning eller ett svenskt konsulat om den sökande inte befinner sig i Sverige. Motsvarande regler finns för ansökningar om arbetstillstånd i 5 kap. 8 § utlänningsförordningen. Migrationsverket får vidare ge en svensk beskickning eller ett svenskt konsulat rätt att besluta om nationella viseringar. Även Regeringskansliet (Utrikesdepartementet) får ge en svensk beskickning eller ett svenskt konsulat rätt att bevilja nationella viseringar inom departementets ansvarsområde. Detta framgår av 3 kap. 12 § utlänningsförordningen.

Av 9 kap. 1 § utlänningslagen (2005:716) framgår att Polismyndigheten ansvarar för kontroll av personer enligt kodexen om Schengengränserna. Myndigheten genomför även inre utlänningskontroll med stöd av 9 kap. 9 § utlänningslagen.<sup>13</sup> Polismyndigheten får vidare, enligt 8 kap. 17 § utlänningslagen, i vissa fall besluta om avvisning. Myndigheten verkställer också sina egna beslut om avvisning och i vissa fall även Migrationsverkets beslut om utvisning och avvisning (12 kap. 14 § utlänningslagen). Polismyndigheten får även besluta om förvar eller uppsikt av utlänningar enligt 10 kap. 12–13 §§ utlänningslagen.

### 6.3.2 Bedömning

**Bedömning:** Den personuppgiftsbehandling som Migrationsverket, utlandsmyndigheterna och Polismyndigheten utför inom utlänningsdatalagens tillämpningsområde har en sådan rättslig grund som avses i artikel 6.1 c och e i dataskyddsförordningen.

<sup>12</sup> Se förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 27).

<sup>13</sup> Jfr. artikel 21 i Europaparlamentets och rådets förordning (EG) nr 562/2006 av den 15 mars 2006 om en gemenskapskodex om gränspassage för personer (kodex om Schengengränserna).

Kravet på att det ska finnas en rättslig grund för personuppgiftsbehandlingen är i sak inte något nytt för dataskyddsförordningen. Om behandlingen inte utförs med samtycke av den registrerade måste behandlingen även enligt nuvarande lagstiftning vara nödvändig för vissa syften för att vara tillåten. Dessa syften framgår av 10 § PuL, där punkterna b, d och e motsvarar de rättsliga grunder som framgår av artikel 6.1 c och e i dataskyddsförordningen (rättslig förpliktelse, uppgift av allmänt intresse och myndighetsutövning).

Med mycket få undantag utförs den personuppgiftsbehandling som är nödvändig för att Migrationsverket, utlandsmyndigheterna och Polismyndigheten ska kunna sköta sina uppgifter enligt utlännings- och medborgarskapslagstiftningen utan den registrerades uttryckliga samtycke.<sup>14</sup> Enligt vår mening borde man därmed kunna utgå från att lagstiftaren vid utlänningsdatalagens tillkomst bedömde att den personuppgiftsbehandling som sker med stöd av den lagen har rättsligt stöd i 10 § PuL, och därmed i de rättsliga grunder som nu återfinns i artikel 6.1 c och e i dataskyddsförordningen. Trots detta anser vi att det finns anledning att göra en analys av vilken eller vilka av dataskyddsförordningens rättsliga grunder som utgör stödet för den personuppgiftsbehandling som sker inom utlänningsdatalagens tillämpningsområde.

Som framgår av avsnitt 6.3.1 är Migrationsverkets, utlandsmyndigheternas och Polismyndighetens uppdrag inom utlännings- och medborgarskapsområdet fastställda genom lag eller annan författning. I större delen av verksamheten står den enskilde i ett uppenbart beroendeförhållande till myndigheterna, som har makt att bestämma över den enskildes rättigheter och ibland även att göra ingrepp i hans eller hennes frihet. Denna verksamhet motsvarar därmed den definition av myndighetsutövning som framgår av avsnitt 6.2.2. Som uppenbara exempel kan nämnas Migrationsverkets handläggning av och beslut i ärenden om uppehålls- och arbetstillstånd, statusförklaring och medborgarskap samt motsvarande verksamhet hos utlandsmyndigheterna vad gäller nationella viseringar. Även Polismyndighetens verkställighet av beslut om avvisning eller utvisning och om förvar eller uppsikt är enligt vår mening ett självklart uttryck för myndighetsutövning.

---

<sup>14</sup> Se förarbetena till utlänningsdatalagen (prop. 20015/16:65, s. 37).



Ibland kan dock gränsen för vad som utgör myndighetsutövning vara svårare att dra. Som ett exempel kan nämnas att Migrationsverkets ansvar för mottagandet av asylsökande och andra utlänningar bl.a. innebär att de sökande registreras samt ges möjlighet att bo på en förläggning och till sysselsättning. Denna verksamhet utgör inget tvång mot den enskilde, men resulterar ändå i ett antal beslut som påverkar hans eller hennes liv. Det ligger enligt vår mening därmed nära till hands att betrakta verksamheten som myndighetsutövning. När det gäller den hjälp Migrationsverket bistår den enskilde med i återvändandearenden anser vi dock att bedömningen inte är lika lätt att göra. Återvändandet är förvisso frivilligt, men utgör regelmässigt ett resultat av ett avslagsbeslut som meddelats i verkets myndighetsutövning. Om Migrationsverket gör bedömningen att tvång kommer att behövas för att verkställa beslutet får verket vidare enligt 12 kap. 14 § utlänningslagen lämna över ärendet till Polismyndigheten, som har rätt att använda tvångsmedel vid verkställigheten.

Även för vissa delar av utlandsmyndigheternas verksamhet kan det finnas anledning att fundera över vad som utgör myndighetsutövning. När en utlandsmyndighet endast tar emot en ansökan om främlingspass för att därefter vidarebefordra den till handläggande myndighet innefattar detta enligt vår mening inte myndighetsutövning. För de ansökningar om uppehålls- och arbetstillstånd som utlandsmyndigheten ska utreda anser vi inte att slutsatsen är lika självklar, eftersom ärendets handläggning kan påverka utgången. Man skulle också kunna diskutera om det biträde myndigheten ger till övriga myndigheter i form av exempelvis kontroll av faktauppgifter eller äkthetskontroll av handlingar utgör myndighetsutövning eller inte.

Det finns enligt vår mening emellertid inte någon anledning att låsa fast sig vid vilka delar av myndigheternas verksamhet som utgör myndighetsutövning. Anledningen till detta är följande.

Det övergripande målet för migrationspolitiken är bl.a. att säkerställa en långsiktigt hållbar migrationspolitik som inom ramen för den reglerade invandringen värnar asylrätten, underlättar rörlighet över gränser och främjar en behovsstyrd arbetskrafts-

invandring.<sup>15</sup> Migrationspolitiken kommer till uttryck genom den svenska utlännings- och medborgarskapslagstiftningen. De uppgifter som framgår av denna lagstiftning genomförs av främst Migrationsverket, utlandsmyndigheterna och Polismyndigheten. Mot den bakgrunden anser vi att hela den verksamhet myndigheterna har anförtrotts på utlännings- och medborgarskapsområdet utgör en uppgift av allmänt intresse i dataskyddsförordningens mening. Detta gäller oavsett om stora delar av verksamheten även utgör myndighetsutövning mot enskilda.

Den personuppgiftsbehandling som sker för att myndigheterna på ett rättsäkert sätt ska kunna genomföra de uppgifter de har anförtrotts, måste enligt vår mening vidare anses vara *nödvändig* som ett led i myndigheternas myndighetsutövning och/eller för att utföra uppgiften av allmänt intresse. Det rättsliga stödet för den personuppgiftsbehandling som Migrationsverket, utlandsmyndigheterna och Polismyndigheten utför för att fullgöra sina skyldigheter enligt utlännings- och medborgarskapslagstiftningen står enligt vår mening således att finna i artikel 6.1 e i dataskyddsförordningen.

Under handläggningen av ett ärende vidtar myndigheterna en rad utredningsåtgärder av olika slag. De flesta utförs av myndigheten själv med hjälp av egen personal. Andra, exempelvis DNA-analyser och medicinska åldersbedömningar i Migrationsverkets ärenden om uppehållstillstånd, utförs av externa aktörer. DNA-analyser, som under vissa förutsättningar erbjuds i ärenden om uppehållstillstånd på grund av familjeanknytning, får utföras endast om den sökande har gett sitt skriftliga samtycke (13 kap. 15 § utlänningslagen). En medicinsk åldersbedömning ska vid behov erbjudas en sökande som uppger att han eller hon är ett ensamkommande barn. Inte heller denna åtgärd får utföras utan sökandens skriftliga samtycke (13 kap. 17 och 18 §§ utlänningslagen). Av 4 kap. 21 d § utlänningsförordningen framgår att åldersbedömningarna utförs av Rättsmedicinalverket och att Migrationsverkets underrättelse till Rättsmedicinalverket om att en sådan bedömning ska utföras ska innehålla vissa personuppgifter gällande den sökande, såsom namn, kön och ärendenummer.

---

<sup>15</sup> Se betänkande från Utredningen om migrationsmottagandet 2015 (SOU 2017:12 s. 41) med hänvisning till prop. 2009/10:1 UO081 och prop. 2016/17:01, UO08.

Av förarbetena till utlänningslagens bestämmelser om åldersbedömningar (prop. 2016/17:121 s. 22 f.) framgår att en samtyckeslösning valts dels för att tillgodose asylprocedurdirektivets<sup>16</sup> krav och dels för att regleringen inte ska stå i strid med förbudet mot påtvingade kroppsliga ingrepp i 2 kap. 6 § regeringsformen. Det är enligt vår mening mycket angeläget att särskilja bestämmelser om hur en myndighets verksamhet ska utföras och bestämmelser om den personuppgiftsbehandling som är nödvändig för att genomföra denna verksamhet. Vi bedömer att den rättsliga grunden för behandlingen står att finna i artikel 6.1 e i dataskyddsförordningen även när det gäller åldersbedömningar och DNA-analyser, eftersom behandlingen är nödvändig för att utföra den uppgift av allmänt intresse som anförtrots Migrationsverket inom ramen för utlänningslagstiftningen. Det är alltså inte fråga om att samtycke krävs för behandling av personuppgifter med anledning av att åldersbedömningar eller DNA-analyser genomförs med den enskildes samtycke. Varken lagstiftningens utformning eller dess förarbeten ger stöd för att detta skulle ha varit lagstiftarens avsikt.

De svenska registerförfattningarnas primära ändamålsbestämmelser anses vidare allmänt kunna innefatta även utlämnande av personuppgifter till annan, så länge detta sker för myndighetens eget behov.<sup>17</sup> Detta medför att den personuppgiftsbehandling som utförs av Migrationsverket vid en underrättelse till Rättsmedicinalverket om att en åldersbedömning ska ske, utförs i enlighet med den primära ändamålsbestämmelsen i 11 § 1 utlänningsdatalagen (handläggning av ärenden i verksamhet som rör utlänningars inresa i Sverige).<sup>18</sup> Utlänningsförordningens bestämmelser om vilka personuppgifter som ska finnas med i en sådan underrättelse utgör den sekretessbrytande bestämmelse som möjliggör utlämnandet.

---

<sup>16</sup> Europaparlamentets och rådets direktiv 2013/32/EU av den 26 juni 2013 om gemensamma förfaranden för att bevilja och återkalla internationellt skydd (omarbetning).

<sup>17</sup> Se bl.a. 2014 års utlänningsdatautrednings betänkande (SOU 2015:73 s. 261), förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 38), förarbetena till tullbrottsdatalagen (prop. 2016/17:91 s. 94 f.) och Oman, Särskilda registerförfattningar, Festskrift till Peter Seipel, 2006, s. 699 f.

<sup>18</sup> Även om Migrationsverkets underrättelse skulle innehålla känsliga personuppgifter är behandlingen tillåten enligt utlänningsdatalagens bestämmelser, eftersom känsliga personuppgifter får behandlas för handläggning av ärenden enligt 15 § första stycket 1 utlänningsdatalagen (se vidare avsnitt 12.1.3).

Av 13 § utlänningsdatalagen framgår att det inom lagens tillämpningsområde även är tillåtet att i vissa fall behandla personuppgifter om det är nödvändigt för att tillhandahålla information till bl.a. riksdagen, regeringen, annan myndighet eller enskild. En förutsättning för att uppgifter ska få lämnas ut till annan myndighet eller enskild är att uppgifterna lämnas med stöd av lag eller förordning. 13 § utlänningsdatalagen utgör en sekundär ändamålsbestämmelse, som vi behandlar närmare i kapitel 8. Möjligheten att behandla personuppgifter på detta sätt har emellertid relevans när det gäller att fastställa den rättsliga grunden för den behandling som sker inom utlänningsdatalagens tillämpningsområde.

Ett utlämnande av personuppgifter till enskild med stöd av lag eller förordning innefattar t.ex. sådant utlämnade av uppgifter som sker med stöd av tryckfrihetsförordningen. Dataskyddsförordningens bestämmelser om skydd för personuppgifter hindrar inte att en myndighets allmänna handlingar lämnas ut i enlighet med bestämmelser i den nationella lagstiftningen som tillgodoser allmänhetens rätt att få tillgång till allmänna handlingar, såsom den svenska offentlighetsprincipen. Detta framgår av artikel 86 i dataskyddsförordningen.

Vidare har Datainspektionen tidigare gjort bedömningen att en myndighets skyldighet enligt offentlighetsprincipen utgör en rättslig skyldighet. Rättslig skyldighet är 1995 års dataskyddsdirektivs och personuppgiftslagens motsvarighet till dataskyddsförordningens begrepp rättslig förpliktelse. Mot bakgrund av att myndigheters skyldighet enligt offentlighetsprincipen är en lagreglerad förpliktelse anser vi inte att det finns anledning att göra någon annan bedömning. Den personuppgiftsbehandling som utförs när myndigheterna lämnar ut uppgifter från den löpande verksamheten i enlighet med tryckfrihetsförordningen, utgör således en sådan rättslig förpliktelse som avses i artikel 6.1 c i dataskyddsförordningen.

Ett utlämnande av uppgifter enligt tryckfrihetsförordningen utgör enligt vår mening även en sådan uppgift av allmänt intresse som avses i artikel 6.1 e i dataskyddsförordningen. Myndigheternas skyldighet att lämna ut handlingar är reglerad i lag och den insyn i myndigheternas verksamhet som offentlighetsprincipen bidrar till måste anses vara av intresse för allmänheten.

Samma resonemang bör enligt vår mening kunna föras när det gäller annat utlämnande av uppgifter som är reglerat i lag eller förordning. Om lagstiftaren har ansett att en skyldighet att lämna ut uppgifter är av sådan vikt att den ska författningsregleras anser vi att det får förutsättas att det handlar om en sådan uppgift av allmänt intresse som avses i artikel 6.1 e i dataskyddsförordningen. Enligt vår uppfattning bör det faktum att skyldigheten är författningsreglerad också innebära att den utgör en rättslig förpliktelse enligt artikel 6.1 c i förordningen.

Slutligen kan det övervägas om det i utlänningsdatalagen ska tas in en hänvisning till 2 kap. 3 och 4 §§ dataskyddslagen. Det som talar för att en sådan hänvisning bör göras är att det i annat fall skulle kunna uppstå föreställningar om att innehållet i dessa bestämmelser inte är tillämpligt för den personuppgiftsbehandling som sker med stöd av utlänningsdatalagen. Dataskyddslagens krav på rättslig grund för behandlingen är dock endast ett införlivande av en direkt tillämplig bestämmelse i dataskyddsförordningen. Den får således enligt vår mening ses som en upplysningsbestämmelse utan egen rättsverkan. Vi kommer också att föreslå att utlänningsdatalagen ska innehålla en upplysning om att denna lag innehåller kompletterande bestämmelser till dataskyddsförordningen (se avsnitt 9.2). Mot den bakgrunden anser vi att det i utlänningsdatalagen inte behöver eller bör tas in en hänvisning till 2 kap. 3 och 4 §§ dataskyddslagen.

Det faktum att personuppgiftsbehandlingen inom utlänningsdatalagens område – såväl inom ramen för den löpande verksamheten som vid utlämnande av uppgifter som omfattas av lagen – vilar på flera av de rättsliga grunder som anges i artikel 6.1 i dataskyddsförordningen, innebär naturligtvis inte att personuppgifter får behandlas på vilket sätt som helst i denna verksamhet. Dataskyddsförordningens allmänna principer för personuppgiftsbehandling måste alltid följas (se avsnitt 5.2) och i enlighet med det nödvändighetsrekvisit som finns i artikel 6.1 c och e måste frågan om den enskilda personuppgiften är nödvändig att behandla för utförandet av den aktuella verksamheten avgöras för varje enskild behandling. En annan sak är att vissa kategorier av personuppgifter alltid kommer att vara nödvändiga att behandla för att vissa delar av verksamheten ska kunna utföras rättsäkert. Som exempel kan nämnas att personuppgifter som på ett tillräckligt säkert sätt

identifierar den person ett ärende berör alltid kommer att vara nödvändiga att registrera i det enskilda ärendet.

# 7 Syfte och tillämpningsområde

## 7.1 Lagens syfte

**Bedömning:** Dataskyddsförordningen föranleder ingen ändring av utlänningsdatalagens inledande syftesbestämmelse.

Enligt 1 § utlänningsdatalagen är syftet med lagen att ge Migrationsverket, Polismyndigheten och utlandsmyndigheterna möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sin verksamhet enligt utlännings- och medborgarskapslagstiftningen. Syftet är också att skydda människor mot att deras personliga integritet kränks vid sådan behandling. Lagens syftesbestämmelse har enligt vår mening ingen självständig rättslig betydelse, eftersom utlänningsdatalagens tillämpningsområdet beskrivs i bl.a. lagens 2 och 3 §§.

Vid tillkomsten av utlänningsdatalagen gjorde regeringen emellertid bedömningen att lagens dubbla syfte borde komma till tydligt uttryck.<sup>1</sup> Mot den bakgrunden och med hänsyn till att dataskyddsförordningen enligt vår mening inte föranleder någon ändring av syftesbestämmelsen anser vi att denna bör finnas kvar i sin nuvarande lydelse.

---

<sup>1</sup> Se förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 38).

## **7.2 Verksamhet som omfattas av tillämpningsområdet**

### **7.2.1 Migrationsverkets och utlandsmyndigheternas verksamhet**

Utlänningsdatalagen gäller vid viss personuppgiftsbehandling i Migrationsverkets och utlandsmyndigheternas verksamhet. Den verksamhet hos dessa myndigheter som omfattas av utlänningsdatalagen regleras uttömmande i lagens 2 § och rör

1. utlänningars inresa i Sverige, i en stat som ingår i Europeiska unionen, i en stat som är ansluten till Europeiska ekonomiska samarbetsområdet eller i Schweiz,
2. utlänningars vistelse eller arbete i Sverige och utresa eller avlägsnande från Sverige,
3. statusförklaring,
4. mottagande av asylsökande och andra utlänningar,
5. bistånd och stöd till utlänningar,
6. svenskt medborgarskap,
7. statlig ersättning för kostnader för utlänningar,
8. bosättning av utlänningar, eller
9. utfärdande av resehandlingar.

I förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 40–42) görs följande förtydliganden gällande det tillämpningsområde som kommer till uttryck i 2 §.

Med utlänningars inresa, vistelse och arbete (punkt 1 och 2) avses Migrationsverkets verksamhet enligt utlänningslagen (2005:716) och utlänningsförordningen (2006:97), dvs. verksamhet som rör visering, uppehålls- och arbetstillstånd, avvisning eller utvisning, kontroll samt verkställighet av beslut. Även utlandsmyndigheternas biträde vid utredning i Migrationsverkets utlännings- och medborgarskapsärenden med stöd av förordningen (2014:115) med instruktion för utrikesrepresentationen avses. Detsamma gäller Migrationsverkets behandling av personuppgifter i ärenden enligt lagen (1991:572) om särskild utlänningskontroll.



Med utresa eller avlägsnande från Sverige (punkt 2) avses såväl frivillig utresa som utresa efter tvångsverkställighet. I detta begrepp ingår även frågor om förvar och uppsikt.

Verksamhet som rör statusförklaring (punkt 3) avser Migrationsverkets behandling av personuppgifter i anledning av beslut om eller återkallelse av statusförklaring enligt 4 kap. 3–3 c §§ respektive 5 b och 5 c §§ utlänningslagen.

Verksamheten mottagande av asylsökande och andra utlänningar (punkt 4) omfattar Migrationsverkets verksamhet enligt lagen (1994:137) om mottagande av asylsökande m.fl., med undantag för sådan verksamhet som avser ekonomiskt bistånd eller stöd. Migrationsverkets verksamhet i samband med mottagande av kvotflyktingar faller också under denna punkt.

Verksamhet som avser bistånd och stöd till utlänningar (punkt 5) innefattar Migrationsverkets verksamhet med ekonomiskt bistånd enligt lagen om mottagande av asylsökande m.fl.. Hit hör även Migrationsverkets verksamhet enligt förordningen (1984:890) om bidrag till utlänningars resor från Sverige för bosättning i annat land, förordningen (1984:936) om bidrag till flyktingar för kostnader för anhörigs resor till Sverige, förordningen (2008:778) om återetableringsstöd för vissa utlänningar och förordningen (2010:1345) om särskild dagersättning till vissa nyanlända invandrare som vistas vid mottagningsenhet. Den personuppgiftsbehandling hos Migrationsverket som föranleds av bidragsbrottslagen (2007:612) och lagen (2008:206) om underrättelseskyldighet vid felaktiga utbetalningar från välfärdssystemen omfattas också.

Verksamhet som rör svenskt medborgarskap (punkt 6) omfattar Migrationsverkets och utlandsmyndigheternas verksamhet enligt lagen (2001:82) om svenskt medborgarskap och medborgarskapsförordningen (2001:218).

Under delmomentet statlig ersättning för kostnader för utlänningar (punkt 7) faller bl.a. Migrationsverkets personuppgiftsbehandling i samband med handläggning enligt förordningen (1990:927) om statlig ersättning för flyktingmottagande m.m., förordningen (2010:1122) om statlig ersättning för insatser för vissa utlänningar, förordningen (1996:1357) om statlig ersättning för hälso- och sjukvård till asylsökande och förordningen (2002:1118) om statlig ersättning för asylsökande m.fl..

I verksamhet som rör bosättning av utlänningar (punkt 8) ingår Migrationsverkets ansvar för bosättning av vissa utlänningar enligt lagen om mottagande av asylsökande m.fl. Även verkets verksamhet enligt förordningen (2010:408) om mottagande för bosättning av vissa nyanlända invandrare avses.

Verksamhet som rör utfärdande av resehandlingar (punkt 9) är avsedd att omfatta ärenden om främlingspass och andra resehandlingar.

### 7.2.2 Polismyndighetens verksamhet

Utlänningsdatalagen är enligt 3 § tillämplig på den personuppgiftsbehandling som utförs av Polismyndigheten i verksamhet som rör utlänningars inresa och vistelse i Sverige samt utresa eller avlägsnande från Sverige. En förutsättning för detta är dock att verksamheten inte utgör brottsbekämpande verksamhet. Den personuppgiftsbehandling som utförs i den sistnämnda verksamheten regleras i stället genom polisdatalagen (2010:361).

Även Polismyndighetens verksamhet i frågor om förvar och uppsikt inkluderas i den verksamhet som rör utlänningars utresa och avlägsnande.<sup>2</sup> Av förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 33) framgår vidare att den verksamhet hos Polismyndigheten som kan omfattas av tillämpningsområdet i 3 § utlänningsdatalagen bl.a. består av registrering i den s.k. U-boken, i personefterlysningregistret och i fingeravtrycks- och signalementsregistret.

U-boken innehåller information om de personer som i Sverige fått lagakraftvunna avvisnings- och utvisningsbeslut med återreseförbud meddelade mot sig. I personefterlysningregistret registreras utlänningar som Polismyndigheten beslutat att efterlysa för att de inte varit tillgängliga när ett beslut om avvisning eller utvisning ska verkställas. I Polismyndighetens fingeravtrycks- eller signalementsregister får uppgifter behandlas om bl.a. personer som har lämnat fingeravtryck enligt 19 § lagen (1991:572) om särskild utlänningskontroll.

---

<sup>2</sup> Se förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 43).

### 7.2.3 Avgränsning mot direktivsstyrd verksamhet

EU:s dataskyddsreform kommer att innebära förändringar i det svenska regelverket för personuppgiftsbehandling (se kapitel 4). Utredningen om 2016 års dataskyddsdirektiv har i sitt delbetänkande (SOU 2017:29) föreslagit att den nya brottsdatalagen ska vara tillämplig vid behandling av personuppgifter som behöriga myndigheter utför för vissa syften. Dessa syften är att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Även behandling av personuppgifter i syfte att upprätthålla allmän ordning och säkerhet kommer enligt förslaget att omfattas av brottsdatalagen. Utifrån Utredningen om 2016 års dataskyddsdirektivs beskrivning i dess delbetänkande (SOU 2017:29 s. 20), är det rimligt att anta att det även fortsättningsvis kommer att finnas en registerförfattning för Polismyndigheten. Registerförfattningen kommer dock i så fall att innehålla kompletterande bestämmelser till brottsdatalagen.

Utlänningsdatalagen omfattar den behandling av personuppgifter i Polismyndighetens verksamhet som rör utlänningars inresa och vistelse i Sverige samt utresa eller avlägsnande från Sverige. Därmed aktualiseras frågan om Polismyndighetens personuppgiftsbehandling i ärenden om förvar respektive vid utlänningskontroll faller under brottsdatalagens eller dataskyddsförordningens tillämpningsområde.

Utredningen om 2016 års dataskyddsdirektiv har i sitt delbetänkande (a.a. s. 192 f.) gjort bedömningen att brottsdatalagen som huvudregel inte är tillämplig när det gäller personuppgiftsbehandling beträffande någon som har placerats i häkte för annat ändamål än för anhållande, häktning eller verkställighet eller ändring av påföljd. Resonemanget borde enligt vår mening kunna tjäna som ledning även för Polismyndigheten när det gäller den personuppgiftsbehandling som utförs i de förvarsärenden där Polismyndigheten är handläggande myndighet.

När det gäller gränskontroll har Utredningen om 2016 års dataskyddsdirektiv sammanfattningsvis gjort följande bedömning (a.a. s. 199 och 202 f.). Gränskontroll kan inte generellt hänföras till brottsbekämpning eller ordningshållning. Det går dock inte heller att säga att den alltid ligger utanför brottsdatalagens tillämpningsområde. Det krävs därför en bedömning av syftet med

behandlingen av personuppgifter i det enskilda fallet för att avgöra vilket regelverk som ska tillämpas. Utgångspunkten bör vara att det är först när det i kontrollverksamheten finns anledning att anta att ett konkret brott har begåtts eller att någon utövar viss brottslig verksamhet som verksamheten övergår till att bli brottsbekämpande och brottsdatalagen blir tillämplig.

Migrationsverket och utlandsmyndigheterna har inte något uttryckligt brottsbekämpande uppdrag (jfr avsnitt 6.3.1). Enligt 6 § bidragsbrottslagen har Migrationsverket emellertid en skyldighet att anmäla till Polismyndigheten eller Åklagarmyndigheten om det kan misstänkas att ett brott enligt den lagen har begåtts. Den personuppgiftsbehandling som utförs av verket i samband med en sådan anmälan faller inom utlänningsdatalagens tillämpningsområde (se avsnitt 7.2.1). Samtidigt är syftet med behandlingen att gärningen ska kunna utredas och lagföras. Utredningen om 2016 års dataskyddsdirektiv har i sitt delbetänkande (a.a. s. 185–186) dock gjort bedömningen att om de myndigheter som har skyldighet att anmäla misstanke om brott varken har ett brottsbekämpande uppdrag eller annars har anförtrotts myndighetsutövning på det området är de inte behöriga myndigheter i brottsdatalagens mening. De ska därför inte tillämpa den lagen. Den personuppgiftsbehandling Migrationsverket utför i denna del bör därmed även fortsättningsvis omfattas av utlänningsdatalagens tillämpningsområde. Även vad gäller de övriga verksamheter hos Migrationsverket som omfattas av utlänningsdatalagen gör vi bedömningen att de inte utförs för att bekämpa brott eller för något annat av de syften som faller under brottsdatalagens tillämpningsområde. Inte heller utlandsmyndigheternas verksamhet enligt utlännings- och medborgarskapslagstiftningen utförs enligt vår mening i sådant syfte.

#### 7.2.4 Bedömning

**Förslag:** Utlänningsdatalagens bestämmelse om att lagen inte gäller vid behandling av personuppgifter i Polismyndighetens brottsbekämpande verksamhet ska utgå. I stället ska tillämpningsområdet avgränsas på så sätt att lagen inte ska gälla

vid sådan behandling av personuppgifter som omfattas av brottsdatalagens tillämpningsområde.

**Bedömning:** Dataskyddsförordningen föranleder ingen ändring vad gäller vilka delar av Migrationsverkets, Polismyndighetens och utlandsmyndigheternas verksamheter som ska omfattas av utlänningsdatalagens tillämpningsområde.

Medlemsstaternas har, enligt artikel 6.2 i dataskyddsförordningen, möjlighet att utarbeta eller behålla registerförfattningar. Inom ramen för denna möjlighet bör medlemsstaterna kunna bestämma tillämpningsområdet för registerförfattningarna på ett sätt som är lämpligt, så länge förordningens allmänna principer för behandling av personuppgifter följs (se avsnitt 5.3).

De verksamheter hos Migrationsverket och utlandsmyndigheterna som omfattas av 2 § utlänningsdatalagen är väl definierade i förarbetena. Dataskyddsförordningen föranleder ingen ändring av tillämpningsområdet i denna del. Utlänningsdatalagen bör därför även framöver gälla vid personuppgiftsbehandling i de verksamheter hos Migrationsverket och utlandsmyndigheterna som anges i 2 § utlänningsdatalagen.

Som framgår i föregående avsnitt gäller utlänningsdatalagen inte för Polismyndighetens brottsbekämpande verksamhet, där i stället polisdatalagen gäller. EU:s dataskyddsreform kommer emellertid att innebära att den generellt tillämpliga brottsdatalagen – kompletterad av en eventuell registerförfattning för polisens verksamhet – kommer att gälla för den personuppgiftsbehandling som utförs i polismyndighetens brottsbekämpande verksamhet. Tillämpningsområdet för brottsdatalagen är dessutom annorlunda beskrivet än det nuvarande ”brottsbekämpande verksamhet” som används i 1 kap. 2 § polisdatalagen och 3 § utlänningsdatalagen. Detta innebär enligt vår mening att utlänningsdatalagens tillämpningsområde måste avgränsas på ett annat sätt än i dag.

Mot den bakgrunden föreslår vi att den del av nuvarande 3 § utlänningsdatalagen som klargör att lagen inte gäller för den brottsbekämpande verksamheten hos Polismyndigheten ska utgå. I stället bör förhållandet mellan utlänningsdatalagen och brottsdatalagen regleras i en ny paragraf i anslutning till nuvarande 2 och 3 §§. Av den nya bestämmelsen bör framgå att utlänningsdatalagen inte

gäller vid sådan behandling av personuppgifter som omfattas av brottsdatalagens tillämpningsområde. Förändringen är främst avsedd att ersätta den befintliga avgränsningen mot Polismyndighetens brottsbekämpande verksamhet med en skrivning som på ett bättre sätt åskådliggör det nya regelverket för personuppgiftsbehandling. Bestämmelsen skulle dock även fungera som en avgränsning mot brottsdatalagens tillämpningsområde om någon verksamhet hos Migrationsverket eller utlandsmyndigheterna i framtiden – pga. ny praxis eller nya arbetsuppgifter – skulle anses falla under brottsdatalagens tillämpningsområde.

## 7.3 Avgränsningar för tillämpningsområdet

### 7.3.1 Lagen om Schengens informationssystem, Viseringskodexen och Eurodac-förordningen

**Bedömning:** Dataskyddsförordningen föranleder ingen ändring vad gäller avgränsningen av utlänningsdatalagens tillämpningsområde mot lagen (2000:344) om Schengens informationssystem, Europaparlamentets och rådets förordning (EG) nr 810/2009 (viseringskodex) eller Europaparlamentets och rådets förordning (EU) nr 603/2013 (Eurodac-förordningen).

För viss personuppgiftsbehandling som myndigheterna utför på utlännings- och medborgarskapsområdet finns regler i annan lagstiftning eller i direkt tillämpliga EU-förordningar. För att undvika dubbelreglering och se till att det inte införs reglering som står i strid med dessa EU-förordningar har det i 5 § utlänningsdatalagen gjorts undantag från tillämpningsområdet för personuppgiftsbehandling som sker med stöd av vissa andra regelverk.<sup>3</sup> Enligt bestämmelsen gäller utlänningsdatalagen inte när personuppgifter behandlas med stöd av

1. lagen (2000:344) om Schengens informationssystem,

---

<sup>3</sup> Se förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 43–44).

2. Europaparlamentets och rådets förordning (EG) nr 810/2009 av den 13 juli 2009 om införande av en gemenskapskodex om viseringar (viseringskodex), eller
3. Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodacuppgifter för brottsbekämpande ändamål, samt om ändring av förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (omarbetning).

Enligt 1 § lagen (2000:344) om Schengens informationssystem (punkt 1) ska Polismyndigheten med hjälp av automatiserad behandling föra ett register som ska vara den svenska nationella enheten i Schengens informationssystem (förkortat SIS). I SIS-registret kan varje Schengenstat föra in uppgifter om personer eller föremål som är efterlysta eller på annat sätt eftersökta med en begäran om att en viss åtgärd ska vidtas när dessa påträffas. SIS innehåller bland annat uppgifter om personer som är efterlysta och begärda utlämnade, en ”spärllista” över utlänningar som ska nekas tillträde till Schengenområdet på grund av utvisningsbeslut eller avvisningsbeslut med förbud att återresa samt uppgifter om försvunna personer.

Den s.k. viseringskodexen (punkt 2) reglerar handläggningen av viseringsansökningar och den s.k. Eurodac-förordningen (punkt 3) behandlar regler om jämförande av fingeravtryck från bl.a. asylsökande.

Som framgår av avsnitt 5.3 anser vi att medlemsstaterna har möjlighet att bestämma tillämpningsområdet för de särskilda registerförfattningar som kompletterar dataskyddsförordningen. I detta ingår naturligtvis även att avgränsa tillämpningsområdet på det sätt som gjorts i 5 § utlämningsdatalagen. Mot den bakgrunden

anser vi att den nuvarande avgränsningen av utlänningsdatalagens tillämpningsområde som kommer till uttryck i 5 § bör finnas kvar.

### 7.3.2 Lagen om passagerarregister

#### Gällande rätt

Europeiska unionens råd antog den 29 april 2004 direktiv 2004/82/EG om skyldighet för transportörer att lämna uppgifter om passagerare, det s.k. API-direktivet.<sup>4</sup> I direktivet regleras flygtransportörers<sup>5</sup> skyldighet att översända förhandsinformation om passagerare (API-uppgifter)<sup>6</sup> till behöriga nationella myndigheter. Syftet med direktivet är att förbättra gränskontrollerna och att bekämpa olaglig invandring. Direktivet utgör också ett led i kampen mot terrorismen.<sup>7</sup>

API-direktivets bestämmelser om transportörers uppgiftsskyldighet har i Sverige genomförts genom bestämmelserna i 9 kap. 3 a–f §§ utlänningslagen (2005:716). Av dessa bestämmelser framgår att det är Polismyndigheten som är behörig att ta emot API-uppgifterna från transportörerna. Av 19 kap. 5 a–8 §§ utlänningslagen framgår vidare att transportörer kan vara skyldiga att betala en särskild avgift om de inte har fullgjort sin uppgiftsskyldighet. Därutöver finns en särskild registerförfattning – lagen (2006:444) om passagerarregister – som reglerar hur Polismyndigheten får behandla de API-uppgifter som transportörerna har fört över till myndigheten. Denna lag innehåller bl.a. bestämmelser om ändamålet med behandlingen, utlämnande av uppgifter, direktåtkomst, rättelse och skadestånd.

#### Bedömning

**Förslag:** Utlänningsdatalagen ska inte gälla när personuppgifter behandlas med stöd av lagen (2006:444) om passagerarregister.

<sup>4</sup> EUT L 261 6.8.2004, s. 24, Celex 32004L0082.

<sup>5</sup> I API-direktivet definieras transportör som en fysisk eller juridisk person som bedriver yrkesmässig persontrafik luftvägen.

<sup>6</sup> Advance Passenger Information.

<sup>7</sup> Se artikel 1 i direktivet samt skäl 2 till detsamma.



Som framgår i föregående avsnitt utförs behandlingen av personuppgifter enligt lagen om passagerarregister delvis i brottsbekämpande syfte. Sådan behandling faller under 2016 års dataskyddsdirektivs och brottsdatalagens tillämpningsområde. Eftersom syftet även är att förbättra gränskontrollerna anser vi dock att personuppgiftsbehandlingen enligt lagen om passagerarregister i vissa delar också faller under dataskyddsförordningens tillämpningsområde.

Lagen om passagerarregister utgör en specialreglering för en viss typ av personuppgifter. Vi gör därmed bedömningen att den gäller före utlänningsdatalagen (*lex specialis*). Det rör sig emellertid om en reglering inom utlänningsrättens område. Av den anledningen kan det, enligt de ställningstaganden som gjorts i tidigare förarbeten (se avsnitt 7.3.1), finnas anledning att i utlänningsdatalagen klargöra förhållandet mellan de båda lagarna. Mot den bakgrunden föreslår vi att det i utlänningsdatalagen ska tas in en bestämmelse som klargör att den lagen inte gäller för personuppgiftsbehandling som utförs med stöd av lagen om passagerarregister. I enlighet med befintlig systematik bör denna bestämmelse föras in som en ny punkt i 5 §, som reglerar de övriga situationer där utlänningsdatalagens bestämmelser inte gäller.

### 7.3.3 VIS-förordningen

#### Gällande rätt

Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS-förordningen) reglerar EU:s gemensamma informationssystem för viseringar. Av artikel 33.3 och artikel 38.2 i VIS-förordningen framgår att den registrerades rätt till skadestånd, korrigering (som motsvarar rättelse) och radering ska regleras i medlemsstaternas nationella rätt.

Enligt artikel 33.1 i VIS-förordningen ska varje person eller medlemsstat som har lidit skada till följd av en otillåten behandling eller av något annat handlade som är oförenligt med bestämmelserna i förordningen ha rätt till ersättning av den medlemsstat som är ansvarig för den uppkomna skadan.

Skadeståndsanspråk mot en medlemsstat för sådana skador ska, enligt artikel 33.3, regleras av svarandemedlemsstatens nationella bestämmelser.

Av artikel 38.2 i VIS-förordningen framgår att var och en får begära att oriktiga uppgifter om honom eller henne korrigeras och att uppgifter som har registerats på olagligt sätt raderas. Korrigering och radering ska utföras utan dröjsmål av den ansvariga medlemsstaten, i enlighet med dess lagar och andra författningar.

För att uppfylla VIS-förordningens krav på nationell reglering finns i 6 § utlänningsdatalagen en bestämmelse som innebär att 28 och 48 §§ PuL om rättelse respektive skadestånd gäller när personuppgifter behandlas med stöd av VIS-förordningen, om inte något annat följer av den förordningen. I övrigt är utlänningsdatalagen inte tillämplig när personuppgifter behandlas med stöd av VIS-förordningen. Skälet till detta är – liksom för viseringskodexen och Eurodac-förordningen – att undvika dubbelreglering och se till att utlänningsdatalagen inte reglerar personuppgiftsbehandling i strid med det unionsrättsliga regelverket.<sup>8</sup>

Som framgår av artikel 33.1 i VIS-förordningen är förordningens krets av skadeståndsberättigade vidare än personuppgiftslagens. Personuppgiftslagens bestämmelse omfattar endast skadestånd till den registrerade, medan även andra personer och medlemsstater kan ha rätt till skadestånd enligt VIS-förordningen. Av förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 45) framgår att regeringen har gjort bedömningen att ett krav på ersättning som framställs av någon som inte är registrerad omfattas av de generella reglerna i skadeståndslagen (1972:207).

När dataskyddsförordningen börjar tillämpas kommer personuppgiftslagen att upphävas.<sup>9</sup> Den generella regleringen för personuppgiftsbehandling kommer då att finnas i dataskyddsförordningen och inte i nationell rätt.

Den registrerades rätt till rättelse och radering av personuppgifter regleras i artikel 16 och 17 i dataskyddsförordningen. Bestämmelser om den registrerades rätt till skadestånd finns i artikel 82 i förordningen och innebär att varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av

---

<sup>8</sup> Se förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 43–44).

<sup>9</sup> Se kommittédirektiv till Dataskyddsutredningen (Dir. 2016:15 s. 6).

förordningen har rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den uppkomna skadan. Bestämmelsen reglerar även bl.a. solidariskt ansvar och regressrätt mellan de ansvariga (se vidare avsnitt 14.8.2).

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) föreslagit att dataskyddslagen ska innehålla en bestämmelse som innebär att rätten till ersättning enligt artikel 82 i dataskyddsförordningen även gäller vid överträdelser av bestämmelser i dataskyddslagen och andra författningar som kompletterar dataskyddsförordningen. Att så är fallet följer redan av skäl 146 till dataskyddsförordningen, där det förtydligas att behandling som strider mot dataskyddsförordningen även omfattar behandling som strider mot medlemsstaternas nationella rätt med närmare specifikation av förordningens bestämmelser. Den föreslagna bestämmelsen i dataskyddslagen är således av klargörande karaktär.<sup>10</sup>

## Bedömning

**Förslag:** När personuppgifter behandlas med stöd av VIS-förordningen ska följande gälla.

1. Den personuppgiftsansvarige är skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med VIS-förordningen. Den personuppgiftsansvarige ska också underätta tredje man till vilken uppgifterna har lämnats ut om åtgärden, om den registrerade begär det eller om mera betydande skada eller olägenhet för den registrerade skulle kunna undvikas genom en underrättelse. Någon sådan underrättelse behöver dock inte lämnas, om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.
2. Den personuppgiftsansvarige ska ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med VIS-förordningen orsakat. Ersättningskyldigheten kan i den utsträckning det

<sup>10</sup> Se Dataskyddsutredningens betänkande (SOU 2017:39 s. 302 f.).

är skäligt jämkas, om den personuppgiftsansvarige visar att felet inte berodde på honom eller henne.

I övrigt ska utlänningsdatalagen även fortsättningsvis inte vara tillämplig när personuppgifter behandlas med stöd av VIS-förordningen.

Utlänningsdatalagen är för närvarande inte tillämplig på den personuppgiftsbehandling som sker med stöd av VIS-förordningen. Dataskyddsförordningen föranleder ingen ändring av detta förhållande, som därmed bör kvarstå oförändrat.

Eftersom personuppgiftslagen kommer att upphävas måste emellertid hänvisningen till den lagens bestämmelser utgå. Frågan är då hur VIS-förordningens krav på en nationell reglering av rätten till rättelse, radering och skadestånd ska hanteras.

Som vi nämnt i föregående avsnitt kommer det när dataskyddsförordningen börjar tillämpas inte att finnas några generellt tillämpliga bestämmelser om rättelse och radering i svensk lagstiftning. Den föreslagna skadeståndsbestämmelsen i dataskyddslagen utgör vidare endast ett förtydligande av hur dataskyddsförordningens bestämmelser om skadestånd ska tolkas.

I brist på nationella bestämmelser att hänvisa till vad gäller rätten till rättelse, radering och skadestånd föreslår vi att det i utlänningsdatalagen införs en reglering, motsvarande den som för närvarande finns i 28 och 48 §§ PuL, som endast gäller för personuppgiftsbehandling enligt VIS-förordningen. En sådan särreglering passar förvisso mindre bra in i utlänningsdatalagens systematik. Det får emellertid ses som en enkel och tillfällig lösning i väntan på en översyn av VIS-förordningen. Alternativet vore att i utlänningsdatalagen föreskriva att dataskyddsförordningens bestämmelser om rättelse, radering och skadestånd gäller vid personuppgiftsbehandling som sker enligt VIS-förordningen. Mot bakgrund av att det av VIS-förordningen framgår att dessa frågor ska regleras i medlemsstaternas nationella rätt förordar vi dock inte denna lösning.

Vi föreslår således att det av utlänningsdatalagen ska framgå att när personuppgifter behandlas med stöd av VIS-förordningen gäller följande.

1. Den personuppgiftsansvarige är skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med VIS-förordningen. Den personuppgiftsansvarige ska också underätta tredje man till vilken uppgifterna har lämnats ut om åtgärden, om den registrerade begär det eller om mera betydande skada eller olägenhet för den registrerade skulle kunna undvikas genom en underrättelse. Någon sådan underrättelse behöver dock inte lämnas, om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.
2. Den personuppgiftsansvarige ska ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med VIS-förordningen orsakat. Ersättningsskyldigheten kan i den utsträckning det är skäligt jämkas, om den personuppgiftsansvarige visar att felet inte berodde på honom eller henne.

I övrigt bör utlänningsdatalagen, liksom i dag, inte vara tillämplig när personuppgifter behandlas med stöd av VIS-förordningen. På samma sätt som i dag bör vidare ett krav på ersättning enligt VIS-förordningen som framställs av någon som inte är registrerad omfattas av de generella reglerna i skadeståndslagen (1972:207).<sup>11</sup>

## 7.4 Automatiserad behandling och manuella register

**Bedömning:** Dataskyddsförordningen föranleder ingen ändring av utlänningsdatalagens bestämmelse om att lagen endast gäller för sådan personuppgiftsbehandling som är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

---

<sup>11</sup> Jfr förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 45).

Utlänningsdatalagen är, enligt 4 §, endast tillämplig på personuppgiftsbehandling som är ”helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier”. Avgränsningen av utlänningsdatalagens tillämpningsområde motsvarar i denna del därmed personuppgiftslagens tillämpningsområde så som det beskrivs i 5 §.

Dataskyddsförordningens materiella tillämpningsområde framgår av artikel 2.1 och beskrivs som ”behandling av personuppgifter som helt eller delvis företas på automatisk väg samt annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register”. Tillämpningsområdet för 2016 års dataskyddsdirektiv beskrivs på liknande sätt i artikel 2.2. Dataskyddsförordningens tillämpningsområde är därmed något annorlunda beskrivet än utlänningsdatalagens.

Av dataskyddsförordningens skäl 15, där förordningens tillämpningsområde berörs, framgår att ”skyddet för fysiska personer bör vara tillämpligt på både automatiserad och manuell behandling av deras personuppgifter, om personuppgifterna ingår i eller är avsedda att ingå i ett register”. I skälen används således begreppet *automatiserad* i stället för *på automatisk väg*. De två uttrycken kan därmed inte gärna uppfattas som annat än synonyma. Vi bedömer därmed att det inte finns någon begreppsskillnad mellan förordningens *på automatisk väg* respektive utlänningsdatalagens *automatiserad*.

Begreppet *automatiserad* har använts i personuppgiftslagen under lång tid och är väl inarbetat även i de svenska registerförfattningarna.<sup>12</sup> Vi anser att det inte finns någon risk för att utlänningsdatalagens tillämpningsområde misstolkas om begreppet får kvarstå. Mot den bakgrunden anser vi att begreppet *automatiserad* bör finnas kvar i utlänningsdatalagen.

Av artikel 4.6 i dataskyddsförordningen framgår att med *register* i förordningens mening avses ”en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på

---

<sup>12</sup> Se bl.a. 1 kap. 2 § andra stycket polisdatalagen (2010:361) och 1 kap. 2 § andra stycket kustbevakningsdatalagen (2012:145)

grundval av funktionella eller geografiska förhållanden”. Samma definition finns i artikel 3.6 i 2016 års dataskyddsdirektiv. Någon saklig skillnad mellan dataskyddsförordningens *register* och utlänningsdatalagens ”strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier” finns enligt vår uppfattning inte, eftersom den avslutande bisatsen i dataskyddsförordningens definition inte ändrar avgränsningen av definitionen i sak.

Trots de något olika uttrycken i dataskyddsförordningen respektive utlänningsdatalagen gör vi bedömningen att förordningens materiella tillämpningsområde i denna del stämmer överens med utlänningsdatalagens nuvarande tillämpningsområde.

Vid införandet av personuppgiftslagen gjordes bedömningen att begreppet *register* är otidsenligt (prop. 1997/98:44 s. 39). Mot den bakgrunden valde lagstiftaren att inte använda begreppet *register*. I stället användes i personuppgiftslagen den längre beskrivning av begreppet *register* som nu också används i utlänningsdatalagen.

När dataskyddsförordningen börjar tillämpas kommer de svenska registerförfattningarna att utgöra en komplettering till förordningen. Man skulle därför kunna argumentera för att begreppet *register* bör användas även i utlänningsdatalagen. Detta skulle kunna undanröja risken för missförstånd och skilda tolkningar av begreppet. Definitionen av *register* i artikel 4.6 i dataskyddsförordningen innehåller vidare, som vi pekat på ovan, ytterligare beskrivningar av begreppet än ”tillgänglighet enligt särskilda kriterier”. En användning av samma begrepp i utlänningsdatalagen skulle innebära att man inte tappar delar av definitionen.

Utredningen om 2016 års dataskyddsdirektiv har dock i sitt betänkande (SOU 2017:29) föreslagit att uttrycket ”strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier” ska användas i brottsdatalagen i stället för begreppet *register*. Detsamma gäller för det nyligen lämnade förslaget till en omarbetad domstolsdatalag.<sup>13</sup> Det är enligt vår mening värdefullt att, så långt det är möjligt, använda samma begrepp i alla de svenska författningar som rör personuppgiftsbehandling. Det uttryck som föreslagits för bl.a. brottsdatalagen är dessutom väl inarbetat i svensk rätt genom bl.a.

---

<sup>13</sup> Ds 2017:41 s. 90 ff.

personuppgiftslagen och ett flertal registerförfattningar. Mot den bakgrunden föreslår vi att utlänningsdatalagens tillämpningsområde ska vara oförändrat även i denna del.



# 8 Ändamålsbestämmelser

## 8.1 Primära ändamålsbestämmelser

### 8.1.1 Rättslig reglering

Av artikel 5.1 b i dataskyddsförordningen framgår att personuppgifter endast får samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Detta kallas för ändamålsbegränsning och det senare ledet benämns ofta finalitetsprincipen (se avsnitt 8.4). Motsvarande bestämmelse finns i artikel 6.1 b i 1995 års dataskyddsdirektiv och har införts i svensk rätt genom 9 § första stycket c och d PuL. Utlänningsdatalagen hänvisar till personuppgiftslagens bestämmelser genom 8 § första stycket 3.

Registerförfattningarnas ändamålsbestämmelser brukar delas upp i primära och sekundära ändamål. Bestämmelserna om primära ändamål tillgodoser den berörda myndighetens eget behov av att behandla personuppgifter. Bestämmelser om sekundära ändamål reglerar i vilken utsträckning uppgifter som samlats in för myndighetens egen verksamhet får behandlas för att lämnas ut till enskilda eller till andra myndigheter i syfte att tillgodose deras behov.<sup>1</sup>

Utlänningsdatalagens primära ändamålsbestämmelser finns i 11 och 12 §§. Enligt 11 § får Migrationsverket, Polismyndigheten och utlandsmyndigheterna behandla personuppgifter om det behövs för

1. handläggning av ärenden eller en myndighets biträde i sådana ärenden i verksamhet som avses i 2 och 3 §§,

---

<sup>1</sup> Se 2014 års utlänningsdatautrednings betänkande (SOU 2015:73 s. 261).

2. kontroll av utlännning i samband med inresa och utresa samt kontroll under vistelsen i Sverige,
3. utförande av arbetsuppgifter som gäller mottagande och bosättning av asylsökande och andra utlännningar,
4. framställning av statistik,
5. utförande av testverksamhet, eller
6. fullgörande av en rättslig skyldighet att registrera eller på annat sätt dokumentera en personuppgift.

Enligt 12 § utlänningsdatalagen får Migrationsverket därutöver också behandla personuppgifter om det behövs för återsökning av avgöranden, rättsutredningar och annan rättslig information eller om det behövs för återsökning av information som rör förhållanden i andra länder.

Av förarbetena till utlänningsdatalagen (SOU 2015:73 s. 266 och prop. 2015/16:65 s. 57) framgår att utlänningsdatalagens primära ändamålsbestämmelser är uttömmande.

### 8.1.2 Tidigare förarbeten

Regeringen konstaterade i förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 60 ff.) att lagrådet i tidigare lagstiftningsärenden har framfört att en ändamålsbestämmelse som tar sikte på en myndighets planering, uppföljning och utvärdering av verksamheten är obehövlig. Lagrådet ansåg att sådan verksamhet är en integrerad del av själva verksamheten och inte någon fristående aktivitet som behöver regleras särskilt. Mot den bakgrunden har det för utlänningsdatalagen inte föreslagits någon särskild reglering som innebär att personuppgiftsbehandling för tillsyn, kontroll, uppföljning eller planering av verksamheten är tillåten. Därutöver angav regeringen i förarbetena sammanfattningsvis följande angående innebörden av utlänningsdatalagens primära ändamålsbestämmelser.

## Handläggning av ärenden m.m.

Begreppet handläggning bör ges en vid tolkning och innefatta alla moment som kan bli aktuella vid handläggningen av ett ärende. Till exempel bör ändamålet omfatta Migrationsverkets behandling av personuppgifter i samband med mottagande, registrering och beredning av ärenden, förordnande av offentligt biträde, kommunikation med den sökande, kommunikation med andra tjänstemän inom samma myndighet med anledning av ärendet samt upprättande och meddelande av beslut.

Ändamålet bör även omfatta Polismyndighetens personuppgiftsbehandling i kontroll- och verkställighetsärenden. Till sådan verksamhet hör till exempel att Polismyndigheten på elektronisk väg får tips om var personer som ska utvisas befinner sig eller att myndigheten själv använder sig av automatiserad behandling i syfte att identifiera och hitta personer vars beslut om avlägsnande Polismyndigheten ska verkställa. Även den personuppgiftsbehandling som utförs i samband med Polismyndighetens verkställande av Migrationsverkets beslut om förvar bör falla under detta ändamål. Ändamålet bör slutligen ge stöd för utlandsmyndigheternas personuppgiftsbehandling i den medverkan till utredning i Migrationsverkets, Polismyndighetens och Säkerhetspolisens handläggning av utlännings- och medborgarskapsärenden som sker med stöd av förordningen (2014:115) med instruktion för utrikesrepresentationen. Ändamålet bör vidare tolkas så att det ger stöd för att personuppgifter som samlats in för ett visst ärende behandlas i ett senare ärende som rör samma person eller i ett ärende som rör en annan person men där den registrerade förekommer som exempelvis anhörig.

## Kontroll av utläningar

Polismyndigheten har behov av att utföra personuppgiftsbehandling i samband med yttre gränskontroll och inre utlänningskontroll. Migrationsverket kan också medverka vid sådan kontrollverksamhet. När den kontroll som Polismyndigheten bedriver inte har brottsbekämpande syfte, är ändamålet att kontrollera den inresandes identitet och att kontrollera att han eller hon uppfyller de formella och materiella kraven enligt utlänningslagen för rätt till

inresa och vistelse i Sverige. I sådana fall regleras personuppgiftsbehandlingen av utlänningsdatalagen.

### **Mottagande och bosättning**

Särskilda bestämmelser om Migrationsverkets ansvar vid mottagande och bosättning av asylsökande och andra utlänningar finns bl.a. i lagen (1994:137) om mottagande av asylsökande m.fl. Ändamålet möjliggör personuppgiftsbehandling hos Migrationsverket som avser ombesörjandet av boende och sysselsättning för asylsökande och andra utlänningar, men som inte direkt utförs inom ramen för ett enskilt ärende. Som exempel kan nämnas myndighetens kontakter med arbetsgivare och andra myndigheter för att ordna praktikplats åt en asylsökande. Inom ramen för det nu föreslagna ändamålet faller också myndighetens arbete med att ta emot kvotflyktingar, bl.a. vad gäller praktiskt arbete med mottagande och bosättning. Det torde mycket sällan bli aktuellt för Polismyndigheten eller utlandsmyndigheterna att behandla personuppgifter för det nu föreslagna ändamålet. Lagstiftningen är dock utformad för att inte lägga hinder i vägen för nödvändig personuppgiftsbehandling om sådant behov skulle uppkomma.

### **Statistik och testverksamhet**

Som exempel på denna typ av verksamhet nämns Migrationsverkets skyldighet att, enligt förordningen (2007:996) med instruktion för Migrationsverket, föra register och statistik över utlänningar i landet i den utsträckning som behövs för verksamheten. Migrationsverket framställer även statistik till externa mottagare såsom riksdagen, Regeringskansliet, fackförbund, Eurostat och UNHCR. Myndigheterna har också ofta behov av att kunna använda personuppgifter i testverksamhet, t.ex. för att kontrollera att it-systemen fungerar på ett effektivt och rättssäkert sätt eller vid introducerandet av ny teknisk utrustning eller datasystem.

Det kan visserligen hävdas att behandling av personuppgifter för att framställa statistik och bedriva testverksamhet många gånger måste anses ha ett sådant samband med verksamheten i övrigt att den inte skulle behöva regleras i en särskild ändamålsbestämmelse.

Genom att framställning av statistik särskilt omnämns i ändamålsbestämmelsen klargörs emellertid att personuppgifter får behandlas för statistikändamål oavsett om det handlar om att tillgodose den egna myndighetens behov eller om att framställa statistik för att kunna lämna över den till andra myndigheter.

### **Skyldighet att registrera eller dokumentera personuppgifter**

Viss personuppgiftsbehandling är nödvändig utan att den kan sägas direkt röra den konkreta kärnverksamheten enligt utlännings- och medborgarskapslagstiftningen. Exempelvis kan personuppgifter som har lämnats in till myndigheterna utan att ha samband med ett ärende utgöra en del av en allmän handling i tryckfrihetsförordningens mening. Sådana handlingar ska, enligt 5 kap. 1 § OSL, diarieföras så snart som möjligt. I förvaltningslagen (1986:223) finns vissa regler om anteckningsskyldighet, parts rätt att ta del av det som tillförts ärendet och kommunikationsplikt. Även dessa bestämmelser kan innebära att personuppgifter måste behandlas. Med anledning av den uttömmande regleringen av utlänningsdatalagens primära ändamål behövs det en ändamålsbestämmelse som tar sikte på myndigheternas skyldighet att registrera och på annat sätt dokumentera personuppgifter som kommer in till myndigheterna.

### **Migrationsverkets återsökning av avgöranden m.m.**

För Migrationsverket är tillgången till aktuell rättspraxis och uppdaterad information om länder nödvändig för att myndigheten ska kunna fatta korrekta beslut i enlighet med gällande praxis och i övrigt bedriva verksamheten så effektivt och rättssäkert som möjligt. I rättsfallssamlingar är identiteten på en person oftast oväsentlig för informationsvärdet. Däremot kan det vara nödvändigt att behandla titlar på domar från exempelvis EU-domstolen och Europadomstolen även om de innehåller ett namn på en person.

## 8.2 Sekundära ändamålsbestämmelser

### 8.2.1 Rättslig reglering

Utlänningsdatalagens sekundära ändamål anges i 13 §. Enligt bestämmelsens första stycke får personuppgifter som behandlas enligt 11 och 12 §§ även behandlas när det är nödvändigt för att tillhandahålla information till

1. riksdagen eller regeringen,
2. en annan myndighet eller en enskild, om uppgifterna lämnas med stöd av lag eller förordning, eller
3. en utländsk myndighet, ett EU-organ eller en mellanfolklig organisation, om utlämnandet av uppgifterna följer av Sveriges medlemskap i Europeiska unionen eller av uppgiftsskyldighet enligt en internationell konvention som Sverige har tillträtt eller enligt ett av riksdagen godkänt avtal med främmande stat eller mellanfolklig organisation.

De sekundära ändamål som anges i 13 § första stycket utlänningsdatalagen är emellertid inte uttömmande. Enligt 13 § andra stycket utlänningsdatalagen får personuppgifter som behandlas för de primära ändamålen (11 och 12 §§) i ett enskilt fall även behandlas för att tillhandahålla information för något annat ändamål än de som uttryckligen anges i 13 § första stycket. En förutsättning för detta är att ändamålet inte är oförenligt med det ändamål som uppgifterna samlades in för. Den nya behandlingen måste således stå i överensstämmelse med finalitetsprincipen så som den beskrivs i 9 § första stycket d PuL för att vara tillåten.<sup>2</sup> Enligt vad som framgår av 2014 års utlänningsdatautrednings betänkande (SOU 2015:73 s. 266) förefaller bestämmelsens ordalydelse ”i ett enskilt fall” syfta på att det är bedömningen av en behandlings förenlighet med det ursprungliga ändamålet som ska göras i det enskilda fallet. Begränsningen till ”ett enskilt fall” förefaller således inte avse en särskild restriktivitet vad gäller själva användandet av möjligheten att lämna ut uppgifter.

---

<sup>2</sup> Jfr förarbetena till utlänningsdatalagen (SOU 2015:73 s. 266 och 443) samt (prop. 2015/16:65 s. 68).

## 8.2.2 Tidigare förarbeten

Vad gäller utlänningsdatalagens sekundära ändamålsbestämmelser framgår av förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 68 ff.) följande.

### Information till riksdagen, regeringen, annan myndighet eller enskild

Det finns en rad olika författningar som föreskriver en uppgiftsskyldighet för myndigheterna. För det första är myndigheterna i vissa fall skyldiga att lämna ut uppgifter till vissa utpekade myndigheter. Till exempel har Försäkringskassan och Pensionsmyndigheten, enligt 17 kap. 3 § utlänningslagen, rätt att ta del av uppgifter om enskilda hos Migrationsverket. Ett annat exempel är att Migrationsverket ska lämna vissa uppgifter till Centrala studie-stödsnämnden enligt 30 § förordningen (1990:1361) om lån till hemutrustning för flyktingar och vissa andra utlänningar. Av 10 kap. 28 § OSL framgår att sekretess inte hindrar att en uppgift lämnas till en myndighet, om uppgiftsskyldighet följer av lag eller förordning.

Myndigheter är vidare i vissa fall enligt lag eller förordning skyldiga att på begäran lämna ut uppgifter till andra. En myndighet är till exempel enligt reglerna i 2 kap. tryckfrihetsförordningen skyldig att lämna ut personuppgifter som finns i allmänna handlingar, om inte sekretess gäller för uppgifterna. Enligt 6 kap. 5 § OSL ska en myndighet därutöver på begäran av en annan myndighet lämna uppgift som den förfogar över, i den mån hinder inte möter på grund av bestämmelser om sekretess eller av hänsyn till arbetets behöriga gång.

Vidare finns det ett antal författningar med bestämmelser som medför att uppgifter får lämnas ut. Bestämmelserna innebär således inte – till skillnad från de ovan beskrivna – en uppgiftsskyldighet, utan enbart att utlämnande är tillåtet. Ett exempel på en sådan bestämmelse är 10 kap. 15 § OSL, enligt vilken sekretess inte hindrar att uppgift lämnas till regeringen eller riksdagen. Vidare finns i 10 kap. 27 § samma lag en generalklausul som innebär att en sekretessbelagd uppgift får lämnas till en annan myndighet om det

är uppenbart att intresset av att uppgiften lämnas ut har företräde framför det intresse som sekretessen ska skydda.

Myndigheterna lämnar inte enbart ut uppgifter för att tillgodose andras behov. En myndighet kan även lämna ut uppgifter på eget initiativ, till exempel för att kunna utföra en uppgift i den egna verksamheten. Det kan till exempel ske med stöd av 10 kap. 2 § OSL, som anger att sekretess inte hindrar att en uppgift lämnas till en enskild eller till en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Ett annat exempel är 10 kap. 18 § samma lag, som anger att sekretess inte hindrar att en uppgift lämnas till en myndighet, om uppgiften behövs där för förundersökning, rättegång, ärende om disciplinansvar eller skiljande från anställning eller annat rättsligt förfarande vid myndighet mot någon rörande hans eller hennes deltagande i verksamheten vid den myndighet där uppgiften förekommer.

När bestämmelser om uppgiftslämnande har införts i lagstiftningen får det förutsättas att det gjorts en avvägning mellan intresset av att uppgiften lämnas ut och intresset av att skydda enskilda personers integritet, vid vilken man funnit att uppgiften ska eller får lämnas ut.

### **Information till utländska myndigheter och organ**

När det gäller EU-samarbetet är mycket av den personuppgiftshantering som sker reglerad i särskilda förordningar, som gäller som svensk lag. Den aktuella bestämmelsen möjliggör att nödvändigt uppgiftslämnande kan ske i det fall sådana särskilda bestämmelser saknas. Detsamma gäller för uppgiftslämnande som sker med stöd av förpliktelser i konventioner eller av riksdagen godkända avtal med främmande stat eller mellanfolkliga organisationer.

Om sekretess gäller för uppgiften får den, enligt 8 kap. 3 § OSL, inte röjas för en utländsk myndighet eller en mellanfolklig organisation, om inte utlämnande sker i enlighet med särskild föreskrift i lag eller förordning eller om uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt



med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen.

### 8.3 Ett uttryckligt angivet och tydligt ändamål

Av artikel 6.3 andra stycket i dataskyddsförordningen framgår att den nationella rätten kan innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen och att dessa bestämmelser kan innehålla bland annat de enheter till vilka personuppgifterna får lämnas ut och för vilka ändamål samt ändamålsbegränsningar (se avsnitt 5.1). Detta ger enligt vår mening stöd för förekomsten av både primära och sekundära ändamålsbestämmelser i nationella registerförfattningar.

Ändamålet med personuppgiftsbehandlingen måste vara uttryckligt angivet och tillräckligt tydligt. Detta framgår av de allmänna principer som gäller enligt artikel 5.1 b i dataskyddsförordningen och skäl 39 till förordningen. Om ändamålen med personuppgiftsbehandlingen inte har en viss grad av precision är det vidare svårt att bedöma om behandlingen uppfyller den princip om uppgiftsminimering som framgår av artikel 5.1 c i dataskyddsförordningen. Enligt denna princip ska personuppgifterna vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål som de samlades in för. En bedömning av om en uppgift är nödvändig för ett visst ändamål eller hur relevant uppgiften är för ändamålet, är svår att göra om ändamålet inte är tillräckligt tydligt angivet.<sup>3</sup>

### 8.4 Finalitetsprincipen

Som framgår av avsnitt 8.2.1 får de aktuella myndigheterna, enligt 13 § andra stycket utlänningsdatalagen, i vissa fall behandla personuppgifter för att tillhandahålla information om detta inte strider mot finalitetsprincipen. Finalitetsprincipen kommer till uttryck i artikel 6.1 b i 1995 års dataskyddsdirektiv och har införts i svensk

---

<sup>3</sup> Jfr Socialdatautredningens betänkande (SOU 1999:109 s. 156).

rätt genom 9 § d PuL. I dataskyddsförordningen återfinns den i artikel 5.1 b och artikel 6.4.

Enligt artikel 5.1 b i dataskyddsförordningen ska – som vi tidigare nämnt – personuppgifter samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Av bestämmelsen framgår också att personuppgifterna inte senare får behandlas på ett sätt som är oförenligt med dessa ändamål. Det framgår emellertid även att ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 inte ska anses vara oförenliga med de ursprungliga ändamålen.

Nytt för dataskyddsförordningen är att det – av artikel 6.4 – framgår vilka faktorer som kan vara av betydelse för att fastställa om en personuppgiftsbehandling för andra ändamål är förenlig med det ändamål som uppgifterna samlades in för. De faktorer som anges i artikel 6.4 a–e är i sin helhet 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 personuppgifts-ansvarige.
- c) Personuppgifternas art, särskilt huruvida särskilda kategorier av personuppgifter behandlas i enlighet med artikel 9 eller huruvida personuppgifter om fällande domar i brottmål och överträdelser 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.

Av skäl 50 till dataskyddsförordningen framgår dock också att om en personuppgiftsbehandling 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 medlemsstaternas nationella rätt fastställa och närmare ange för vilka uppgifter och syften ytterligare behandling bör betraktas som ”förenlig och laglig”. Tillåtligheten av en vidarebehandling kan således säkerställas genom nationell lagstiftning som reglerar när

sådan vidarebehandling ska vara tillåten (jfr artikel 6.3 andra stycket i dataskyddsförordningen och avsnitt 8.3). En sådan nationell reglering ersätter således, enligt vår mening, den prövning som annars ska göras enligt artikel 5.1 b och 6.4 i dataskyddsförordningen av om ändamålet är förenlighet med det ursprungliga.

## 8.5      **Precisering av rättslig grund eller ändamålsbestämmelser?**

Utredningen om 2016 års dataskyddsdirektiv har i sitt delbetänkande (SOU 2017:29 s. 241 ff.) gjort bedömningen att tillåtna rättsliga grunder för behandling och ändamålsbestämmelser ibland har blandats samman.<sup>4</sup> Detta kan enligt den utredningen leda till att tillämparen förväxlar rättslig grund med ändamål och godtar ett i författning angivet allmänt ändamål som ett särskilt och tillräckligt preciserat ändamål. Som ett exempel nämns bestämmelsen i 2 kap. 7 § polisdatalagen (2010:361). Här anges att Polismyndigheten får behandla personuppgifter för att utföra vissa av sina arbetsuppgifter, t.ex. om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet eller för att utreda eller beivra brott. Utredningen om 2016 års dataskyddsdirektiv ifrågasätter om sådana bestämmelser utgör ändamålsbestämmelser eller om de i stället bör betraktas som en precisering av den rättsliga grunden.

Man kan ställa sig frågan om de ändamålsbestämmelser som finns i 11–13 §§ utlänningsdatalagen snarare utgör en precisering av den rättsliga grund som myndigheternas rätt till personuppgiftsbehandling inom utlänningsdatalagens tillämpningsområde vilar på. Den myndighetsutövning eller uppgift av allmänt intresse (jfr artikel 6.1 e i dataskyddsförordningen) som har anförtratts myndigheterna genom utlännings- och medborgarskapslagstiftningen och som framgår av 2 och 3 §§ utlänningsdatalagen kan ytterligare brytas ner till de primära ändamål som anges i 11 och 12 §§ utlänningsdatalagen. På samma sätt bör det utlämnande som sker i enlighet 13 § utlänningsdatalagen utgöra en uppgift av allmänt intresse eller en rättslig förpliktelse (jfr artikel 6.1 c och e i dataskyddsförordningen).

---

<sup>4</sup> Se även Informationshanteringsutredningens slutbetänkande (SOU 2015:39).

Den verksamhet som myndigheterna har ålagts att utföra är emellertid tydligt avgränsad genom utlännings- och medborgarskapslagstiftningen. Detta får enligt vår mening till följd att den rättsliga grunden och de ändamål som personuppgifter behandlas för ligger varandra nära. Vi anser därför att det inte finns något principiellt hinder mot att behålla de ändamål för behandling som nu finns i utlänningsdatalagen.

## 8.6 Bedömning

**Förslag:** Personuppgifter som har behandlats enligt de primära ändamålsbestämmelserna ska i ett enskilt fall få behandlas för att tillhandahålla information under förutsättning att behandlingen är tillåten enligt artiklarna 5.1 b och 6.4 i dataskyddsförordningen.

**Bedömning:** Dataskyddsförordningen föranleder ingen ändring vad gäller förekomsten av ändamålsbestämmelser i utlänningsdatalagen. Det är inte heller nödvändigt att ytterligare precisera de befintliga ändamålen för behandling.

### 8.6.1 Ändamålen för behandling bör uttryckligen anges

Vi anser att de tillåtna ändamålen för personuppgiftsbehandling även fortsättningsvis bör framgå av utlänningsdatalagen. Skälen för detta är följande.

Enligt utlänningsdatalagens primära ändamålsbestämmelser (11–12 §§) får personuppgifter behandlas om det behövs för ett antal där uppräknade arbetsuppgifter. Den personuppgiftsbehandling som myndigheterna utför inom utlänningsdatalagens tillämpningsområde utgörs dock till den allra största delen av traditionell ärendehandläggning. Även den behandling av personuppgifter som är tillåten hos Migrationsverket för att återsöka avgöranden, rättsutredningar, annan rättslig information eller information som rör förhållanden i andra länder sker enligt vår mening till stor del för att ärendehandläggningen ska bli så rättssäker och effektiv som möjligt. För ärendehandläggningen finns både materiella och

processuella förvaltningsrättsliga regler som styr vilka personuppgifter som ska registreras i ärendet. Denna verksamhet är därmed tydligt avgränsad vad gäller behandlingen av personuppgifter.<sup>5</sup> På detta sätt skiljer sig verksamheten från t.ex. de brottsbekämpande myndigheternas verksamhet, där mer övergripande ändamål riskerar att leda till att personuppgifter behandlas i strid med kraven på ändamålsbegränsning och uppgiftsminimering (artikel 5.1 b och c). Vi anser att detsamma gäller för den behandling av personuppgifter som utförs för att fullgöra en rättslig skyldighet att registrera eller på annat sätt dokumentera en personuppgift, eftersom behandlingen av personuppgifter enligt denna ändamålsbestämmelse förutsätts vara föreskriven i författning.

Vår uppfattning är att det inte heller vad gäller Polismyndighetens och Migrationsverkets verksamhet vid yttre gränskontroll och inre utlänningskontroll finns anledning att utmönstra utlänningsdatalagens ändamålsbestämmelser. Syftet med sådan verksamhet är att kontrollera den inresandes identitet och att han eller hon har rätt att resa in och vistas i Sverige. Det rör sig således även här om ett relativt avgränsat uppdrag. Skulle brottsmisstanke uppstå i samband med denna verksamhet kommer personuppgiftsbehandlingen i stället att ske med stöd av brottsdatalagen (se avsnitt 7.2.3).<sup>6</sup>

Som framförs i förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 63 f.) har framställning av statistik respektive utförande av testverksamhet oftast en naturlig koppling till den operativa verksamheten. Det har inte heller kommit fram något som tyder på att det finns anledning att befara att myndigheterna vid sådan verksamhet kommer att behandla personuppgifter på ett sätt som inte är förenligt med principerna om ändamålsbegränsning och uppgiftsminimering.

Även de sekundära ändamål för personuppgiftsbehandling som är angivna i 13 § första stycket utlänningsdatalagen är avgränsade genom att vidarebehandling i de allra flesta fall endast är tillåten om det är föreskrivet, t.ex. i författning eller enligt en internationell

---

<sup>5</sup> Jfr Öman, Särskilda registerförfattningar, Festskrift till Peter Seipel, 2006, s. 703.

<sup>6</sup> Se även Utredningen om 2016 års dataskyddsdirektivs delbetänkande (SOU 2017:29 s. 199 och 202 f).

konvention. Möjligheten att, enligt bestämmelsens andra stycke, behandla personuppgifter för ytterligare ändamål om det inte strider mot finalitetsprincipen är vidare begränsad till situationer där information ska tillhandahållas.

Vi anser också att en lagreglering av personuppgiftsbehandlingen ändamål ger en tydlighet för både de registrerade och de tjänstemän vid myndigheterna som ska behandla personuppgifterna. Eftersom utlänningsdatalagens primära ändamålsbestämmelser dessutom är avsedda att vara uttömmande kommer det inte att vara upp till enskilda tjänstemän att bedöma om en behandling är förenlig med dataskyddsförordningens bestämmelser. Detta utgör enligt vår mening i sig ett skydd för de registrerades integritet.

Enligt artikel 5.1 b i dataskyddsförordningen måste ändamålen med personuppgiftsbehandlingen vara uttryckligt angivna. För det fall det i utlänningsdatalagen inte anges för vilka ändamål personuppgifter får behandlas måste ändamålet för varje behandling framgå på något annat sätt. Vad gäller handläggningen av specifika ärenden torde ändamålet med behandlingen förvisso framgå av sammanhanget, t.ex. prövning av saken X efter ansökan av Y. Även vad gäller yttre och inre gränskontroll torde det framgå av sammanhanget att syftet med denna är att kontrollera den aktuella personen på det sätt som krävs för att exempelvis fastställa om han eller hon har rätt att resa in eller vistas i Sverige. Det kan dock inte uteslutas att det för vissa av de övriga arbetsuppgifter som omfattas av utlänningsdatalagens primära ändamålsbestämmelser (se avsnitt 8.1.1) skulle krävas en dokumentation av ändamålet med personuppgiftsbehandlingen, t.ex. ett angivande av vad det specifika syftet är med att söka bland avgjorda ärenden eller med en specifik statistiksammanställning. En sådan ordning skulle enligt vår mening utgöra en större administrativ belastning för myndigheterna än den nuvarande.

### **8.6.2 Tillräckligt tydliga och specifika ändamål**

Frågan är då om det finns anledning att se över ändamålsbestämmelsernas utformning eller om de redan nu är så specifikt

och uttryckligt angivna som kan krävas (jfr artikel 5.1 b i dataskyddsförordningen)

Som framgår ovan innehåller 1995 års dataskyddsdirektiv samma reglering om ändamålet för personuppgiftsbehandling som dataskyddsförordningen. Utlänningsdatalagens nuvarande ändamålsbestämmelser har således bedömts utifrån samma krav som nu återfinns i dataskyddsförordningen. Detta innebär att lagstiftaren i och med införandet av utlänningsdatalagen måste ha bedömt att de ändamål som anges i lagen är så uttryckligt angivna och tydliga som krävs enligt unionsrätten.

Utlänningsdatalagens primära ändamålsbestämmelse rymmer vidare en mängd olika arbetsuppgifter, som är av mycket skild karaktär (se avsnitt 8.1.2). Mot bakgrund av den diversifierade verksamhet som omfattas av bestämmelserna i 11 och 12 §§ måste de ändamålsbestämmelser som är avsedda att träffa i stort sett hela denna verksamhet enligt vår mening ha en vid formulering. Vi anser därför att utlänningsdatalagens primära ändamålsbestämmelser är så specifika och tydliga som kan krävas i denna verksamhet. Enligt vår uppfattning vore det vidare olämpligt att i ett försök att skapa tydlighet bryta ner de arbetsuppgifter som framgår av bestämmelserna om primära ändamål i ytterligare delmoment. Detta skulle enligt vår mening i stället riskera att göra lagstiftningen ofullständig och skapa förvirring gällande tillåtligheten av de arbetsuppgifter som inte nämns.

Det får dock inte glömmas bort att personuppgiftsbehandlingen måste behövas respektive vara nödvändig för att vara tillåten. Frågan om huruvida behandlingen av en viss personuppgift är adekvat, relevant och inte för omfattande i ett enskilt ärende eller för en enskild arbetsuppgift (jfr artikel 5.1 c i dataskyddsförordningen) får enligt vår mening bedömas utifrån det enskilda ärendets eller arbetsuppgiftens karaktär. I detta sammanhang kan dock anmärkas att innebörden av begreppen *behövs* respektive *nödvändig* i allt väsentligt torde vara densamma. Av förarbetena till utlänningsdatalagen framgår att avsikten med båda begreppen är att betona att behandling av personuppgifter inte får ske slentrianmässigt. Det framgår också att man valt att använda sig av två olika

begrepp främst för att anpassa terminologin i de primära respektive sekundära ändamålsbestämmelserna till polisdatalagen (2010:361).<sup>7</sup>

Enligt utlänningsdatalagens sekundära ändamålsbestämmelse får personuppgifter som samlats in för att de behövs för de primära ändamålen även behandlas om det behövs för att fullgöra uppgiftslämnande, dels till riksdagen eller regeringen och dels om det är föreskrivet. Enligt artikel 6.3 i dataskyddsförordningen är det möjligt att i nationell rätt reglera för vilka ändamål uppgifter får lämnas ut. Som framgår av tidigare förarbeten till utlänningsdatalagen (prop. 2015/16:65 s. 69) får det också förutsättas att det vid den aktuella lagstiftningens tillkomst har gjorts en avvägning mellan intresset av att uppgiften lämnas ut och intresset av att skydda enskilda personers integritet.

Vi anser att utlänningsdatalagens sekundära ändamålsbestämmelse medverkar till att ge en heltäckande bild av vilken personuppgiftsbehandling som är tillåten inom utlänningsdatalagens tillämpningsområde. Bestämmelsen innebär också att det inte råder några tvivel om att det utlämnande av personuppgifter som sker med stöd av exempelvis författning, internationella konventioner eller avtal som ingåtts med främmande stat är tillåtet även enligt dataskyddsförordningen.

Sammantaget gör vi bedömningen att de ändamål för behandling som uttryckligen anges i utlänningsdatalagen är så tydligt angivna och specifika att någon förändring inte behöver eller bör göras.

### 8.6.3 Uppgifter som har behandlats enligt brottsdatalagen

Utredningen om 2016 års dataskyddsdirektiv har i sitt delbetänkande (SOU 2017:29 s. 292) gjort bedömningen att dataskyddsförordningen – och inte brottsdatalagen – är tillämplig när sådana behöriga myndigheter som avses i brottsdatalagen behandlar personuppgifter för att tillhandahålla dessa till andra myndigheter, om ändamålet med behandlingen ligger utanför brottsdatalagens tillämpningsområde. Som ett exempel kan nämnas när Polismyndigheten enligt tryckfrihetsförordningen lämnar ut handlingar som behandlas i gränskontrollverksamhet i syfte att bekämpa brott

---

<sup>7</sup> Se prop. 2015:16:65 s. 58 ff.



(jfr 11 § 2 utlänningsdatalagen). Personuppgifterna har då primärt behandlats med stöd av brottsdatalagen och Polismyndighetens registerförfattning. Utlämnandet av uppgifterna ska dock bedömas utifrån dataskyddsförordningens bestämmelser.

Enligt vad vi erfarit vid samråd med Utredningen om 2016 års dataskyddsdirektiv kommer den utredningen att ge förslag på en reglering av vilken prövning som ska göras innan personuppgifter, som behandlas med stöd av brottsdatalagen, får behandlas för ändamål utanför den lagens tillämpningsområde. Vi kommer därmed inte att behandla den frågan i vår promemoria.

#### 8.6.4 Hänvisningen till finalitetsprincipen

Den hänvisning till finalitetsprincipen som finns i 13 § andra stycket utlänningsdatalagen tillkom som en ventil, eftersom det inte går att förutse alla de fall då uppgifter bör kunna lämnas ut.<sup>8</sup> Dataskyddsförordningen innebär enligt vår bedömning inte någon förändring vad gäller behovet av en sådan bestämmelse. Vi anser dock att det finns anledning att se över hur hänvisningen till finalitetsprincipen ska utformas. Anledningen till detta är att innebörden av finalitetsprincipen har definierats ytterligare i dataskyddsförordningen; av artikel 6.4 framgår vilka faktorer som kan vara av betydelse för att fastställa om en personuppgiftsbehandling för andra ändamål är förenlig med det ändamål som uppgifterna samlades in för.

Genom en hänvisning i 13 § andra stycket utlänningsdatalagen till artikel 5.1 b och 6.4 i dataskyddsförordningen skulle det enligt vår mening stå klart för tillämparen att den nya behandlingen ska bedömas utifrån finalitetsprincipen i dataskyddsförordningens mening. För det fall bestämmelsen kvarstår i sin nuvarande lydelse anser vi att detta inte framstår som lika självklart. Vi föreslår därför att det av utlänningsdatalagen ska framgå att personuppgifter som har behandlats enligt de primära ändamålsbestämmelserna i ett enskilt fall även får behandlas för att tillhandahålla information för något annat ändamål än de som anges i 13 § första stycket, under

---

<sup>8</sup> Se 2014 års utlänningsdatautrednings betänkande (SOU 2015:73 s. 266).

förutsättning att behandlingen är tillåten enligt artiklarna 5.1 b och 6.4 i dataskyddsförordningen.

## 9 Förhållandet till annan lagstiftning

### 9.1 Förhållandet till personuppgiftslagen

**Förslag:** Utlänningsdatalagens bestämmelse om hur lagen förhåller sig till personuppgiftslagen ska upphävas och samtliga hänvisningar till personuppgiftslagen utgå.

Enligt 7 § utlänningsdatalagen gäller den lagen i stället för personuppgiftslagen, om inte annat anges i 8 §. Den senare bestämmelsen innehåller i sin tur hänvisningar till de bestämmelser i personuppgiftslagen som gäller när personuppgifter behandlas enligt utlänningsdatalagen eller enligt föreskrifter som har meddelats i anslutning till lagen.

När dataskyddsförordningen börjar tillämpas kommer personuppgiftslagen att upphävas.<sup>1</sup> Utlänningsdatalagens bestämmelse om hur lagen förhåller sig till personuppgiftslagen måste därmed upphävas och samtliga hänvisningar till personuppgiftslagen utgå. I avsnitt 9.4 redogör vi för innehållet i utlänningsdatalagens befintliga hänvisningar till personuppgiftslagen och gör en bedömning av om dessa ska ersättas.

### 9.2 Förhållandet till dataskyddsförordningen

**Förslag:** Det ska framgå av utlänningsdatalagen att lagen innehåller kompletterande bestämmelser till EU:s dataskyddsförordning.

<sup>1</sup> Se kommittédirektiv till Dataskyddsutredningen (Dir 2016:15 s. 6).

**Bedömning:** Hänvisningarna till personuppgiftslagen bör inte generellt ersättas med hänvisningar till motsvarande bestämmelser i dataskyddsförordningen.

När dataskyddsförordningen börjar tillämpas kommer den att vara direkt tillämplig på all personuppgiftsbehandling som sker inom dess materiella och territoriella tillämpningsområde i medlemsstaterna. Det är också i dataskyddsförordningen som de grundläggande bestämmelserna för personuppgiftsbehandling kommer att finnas. Dessa bestämmelser gäller på utlänningsdatalagens tillämpningsområde oberoende av om förhållandet till förordningen regleras i utlänningsdatalagen. För att uppmärksamma förhållandet mellan dataskyddsförordningen och utlänningsdatalagen och för att underlätta för tillämparen anser vi dock att det bör införas en upplysningsbestämmelse i utlänningsdatalagen som klargör att lagen innehåller kompletterande bestämmelser till dataskyddsförordningen.

Innehållet i flera av personuppgiftslagens bestämmelser kommer framöver att återfinnas i dataskyddsförordningen (se avsnitt 9.4.). Det kan därmed ligga nära till hands att ersätta utlänningsdatalagens hänvisningar till personuppgiftslagen med hänvisningar till dataskyddsförordningens motsvarande bestämmelser. Hänvisningar endast till vissa av förordningens bestämmelser – som dessutom är förhållandevis komplexa – riskerar dock enligt vår mening att skapa otydlighet för tillämparen. Det finns även en risk för missuppfattningen att de bestämmelser i dataskyddsförordningen som utlänningsdatalagen inte hänvisar till inte är tillämpliga. Vi anser generellt sett därför att hänvisningarna till personuppgiftslagen inte bör ersättas med hänvisningar till motsvarande bestämmelser i dataskyddsförordningen.

## Hänvisningsteknik

Vi föreslår i vår promemoria emellertid att vissa bestämmelser i utlänningsdatalagen ska innehålla hänvisningar till bestämmelser i dataskyddsförordningen, t.ex. när det finns möjlighet och anledning att göra undantag från dataskyddsförordningens

bestämmelser (se bl.a. kapitel 14). Sådana hänvisningar kan vara 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.

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39 s. 80 f.) gjort bedömningen att den föreslagna dataskyddslagens hänvisningar till dataskyddsförordningen ska vara dynamiska. Undantaget är en bestämmelse som rör behandling av personuppgifter utanför dataskyddsförordningens egentliga tillämpningsområde. Vi anser att även utlänningsdatalagens hänvisningar till dataskyddsförordningen bör omfatta eventuella framtida ändringar av dataskyddsförordningen och således vara dynamiska. Skälen till detta är följande.

I vårt förslag till 13 a § utlänningsdatalagen finns en hänvisning till artikel 89.1 i dataskyddsförordningen. Hänvisningen har föreslagits för att klargöra att sådana säkerhetsåtgärder som framgår av den senare bestämmelsen krävs för att bl.a. behandling för arkivändamål ska vara tillåten. Eftersom sådana säkerhetsåtgärder är ett krav som framgår av dataskyddsförordningen bör hänvisningen enligt vår mening gälla även för det fall förordningen ändras i denna del.

Den föreslagna ändringen av 15 § utlänningsdatalagen hänvisar till den definition av begreppet *känsliga personuppgifter* som finns i dataskyddsförordningen. Hänvisningen föreslås bl.a. för att anpassa utlänningsdatalagen till dataskyddsförordningens terminologi. Det ter sig enligt vår mening därmed naturligt att en eventuell ändring av dataskyddsförordningens begrepp får genomslag även i utlänningsdatalagen. Detsamma gäller för den ändring vi föreslagit i 13 § andra stycket utlänningsdatalagen, som knyter an till dataskyddsförordningens definition av finalitetsprincipen. Även vad gäller vårt förslag till ändring av 21 § andra stycket utlänningsdatalagen gör sig detta resonemang gällande. Denna bestämmelse klargör att vissa tredjelandsöverföringar av personuppgifter får ske även om det inte finns något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder enligt dataskyddsförordningens bestämmelser.

Slutligen innehåller den föreslagna 18 a § utlänningsdatalagen undantag från den registrerades rätt att enligt dataskydds-

förordningen få information om en personuppgiftsincident. Vi anser att undantaget bör gälla även om det genomförs mindre ändringar i dataskyddsförordningen. Skulle större ändringar genomföras kan valet av en dynamisk hänvisning dock innebära att en översyn av den svenska regleringen behöver göras.

### 9.3 Förhållandet till dataskyddslagen

**Förslag:** Utlänningsdatalagen ska inom sitt tillämpningsområde gälla i stället för den föreslagna dataskyddslagen.

Det ska i utlänningsdatalagen särskilt anges vilka bestämmelser i dataskyddslagen som ska gälla på utlänningsdatalagens tillämpningsområde.

Dataskyddslagen kommer enligt Dataskyddsutredningens förslag att innehålla de författningsbestämmelser som på ett generellt plan kompletterar dataskyddsförordningen.<sup>2</sup> Dataskyddsutredningen föreslår att dataskyddslagen, i likhet med personuppgiftslagen, ska vara subsidiär i förhållande till bestämmelser om behandling av personuppgifter i andra författningar.

Liksom vad som för närvarande gäller i förhållande till personuppgiftslagen, anser vi att utlänningsdatalagen helt ska ersätta dataskyddslagen inom sitt tillämpningsområde. På detta sätt blir regleringen tydlig och bestämmelserna i utlänningsdatalagen måste inte först jämföras med bestämmelserna i dataskyddslagen för att det ska kunna fastställas vilka bestämmelser som är tillämpliga i ett enskilt fall.<sup>3</sup> Vi föreslår därför att det i utlänningsdatalagen ska införas en bestämmelse som reglerar att den lagen gäller i stället för dataskyddslagen, om inte annat anges. Det ska i samband med den bestämmelsen hänvisas till de bestämmelser i dataskyddslagen som ska gälla på utlänningsdatalagens tillämpningsområde.

---

<sup>2</sup> Se Dataskyddsutredningens betänkande (SOU 2017:39).

<sup>3</sup> Jfr förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 46 f.).

## **9.4 Befintliga hänvisningar till personuppgiftslagen och hänvisningar till dataskyddslagen**

### **9.4.1 Definitioner**

I 8 § första stycket 1 utlänningsdatalagen finns en hänvisning till 3 § PuL, som behandlar definitioner. När dataskyddsförordningen börjar tillämpas kommer de definitioner som är aktuella för utlänningsdatalagen att finnas i artikel 4 i förordningen. Mot bakgrund av vårt ställningstagande om hänvisningar till enskilda bestämmelser i dataskyddsförordningen anser vi att någon hänvisning till förordningens bestämmelse inte bör göras i denna del.

### **9.4.2 Förhållandet till offentlighetsprincipen**

I 8 § första stycket 2 utlänningsdatalagen finns en hänvisning till 8 § PuL. Första stycket i den sistnämnda bestämmelsen behandlar förhållandet till offentlighetsprincipen. Vad gäller andra stycket, som bl.a. behandlar arkivering, finns våra överväganden i kapitel 17.

När dataskyddsförordningen börjar tillämpas kommer förhållandet mellan offentlighetsprincipen och regelverket för personuppgiftsbehandling inom dataskyddsförordningens tillämpningsområde att regleras direkt av artikel 86 i förordningen. I denna artikel anges att personuppgifter i allmänna handlingar som förvaras av en myndighet, 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. Det anges vidare att syftet är att jämka samman allmänhetens rätt att få tillgång till allmänna handlingar med rätten till skydd av personuppgifter i enlighet med dataskyddsförordningen.

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39 s. 130) gjort bedömningen att artikel 86 i dataskyddsförordningen innebär att den svenska offentlighetsprincipen har företräde framför dataskyddsförordningen avseende bl.a. handlingar som förvaras hos myndigheter och andra offentliga organ. Frågan om offentlighetsprincipens förhållande till regelverket kring

personuppgiftsbehandling regleras därmed fullt ut genom dataskyddsförordningen. Mot bakgrund av vårt tidigare ställningstagande anser vi att någon hänvisning till dataskyddsförordningens bestämmelse inte bör göras i denna del.

### 9.4.3 Grundläggande krav på behandling av personuppgifter

I 8 § första stycket 3 utlänningsdatalagen finns en hänvisning till 9 § PuL, vars första stycke behandlar grundläggande krav på behandling av personuppgifter. Vad gäller andra, tredje och fjärde stycket, som bl.a. behandlar arkivering, finns våra överväganden i kapitel 17.

Artikel 5 i dataskyddsförordningen innehåller de grundläggande principer för behandling av personuppgifter som kommer att gälla när förordningen börjar tillämpas (se vidare avsnitt 5.2). Mot bakgrund av vårt tidigare ställningstagande anser vi att någon hänvisning till dataskyddsförordningens bestämmelse inte bör göras i denna del.

### 9.4.4 Behandling av personnummer och samordningsnummer

**Förslag:** Uppgifter om personnummer eller samordningsnummer ska även fortsättningsvis 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. Regleringen ska genomföras genom en hänvisning i utlänningsdatalagen till den föreslagna 3 kap. 13 § dataskyddslagen.

I 8 § första stycket 4 utlänningsdatalagen finns en hänvisning till 22 § PuL. Enligt den bestämmelsen får uppgifter om personnummer eller samordningsnummer 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.



Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) föreslagit att 3 kap. 13 § dataskyddslagen ska innehålla en bestämmelse som till sin lydelse helt motsvarar 22 § PuL. Vi föreslår att det i utlänningsdatalagen införs en hänvisning till dataskyddslagens bestämmelse i denna del. På så sätt behålls den reglering av användandet av personnummer och samordningsnummer som tidigare ansetts vara ändamålsenlig inom utlänningsdatalagens tillämpningsområde.

#### **9.4.5 Information till den registrerade och rättelse**

I 8 § första stycket 5 och 6 utlänningsdatalagen finns hänvisningar till 23 och 25–28 §§ PuL. Dessa bestämmelser reglerar information till den registrerade och den registrerades rätt till rättelse, blockering och utplåning av personuppgifter. I kapitel 14 redogör vi för vad som kommer att gälla i dessa frågor när dataskyddsförordningen börjar tillämpas. Där finns även våra överväganden av vilka hänvisningar som bör göras till dataskyddslagen i denna del.

#### **9.4.6 Säkerhet vid behandlingen**

I 8 § första stycket 7 utlänningsdatalagen finns en hänvisning till 30 §, 31 § och 32 § första stycket PuL. Dessa bestämmelser reglerar hur ett personuppgiftsbiträde får behandla personuppgifter, den personuppgiftsansvariges ansvar för att lämpliga skyddsåtgärder vidtas och tillsynsmyndighetens rätt att besluta om säkerhetsåtgärder. Innehållet i 30 och 31 §§ PuL återfinns i delar av artikel 28 och 32 i förordningen. Tillsynsmyndighetens befogenheter regleras i artikel 58 i dataskyddsförordningen. Mot bakgrund av vårt tidigare ställningstagande anser vi att någon hänvisning till dataskyddsförordningens bestämmelser inte bör göras i denna del.

#### **9.4.7 Överföring till tredje land**

I 8 § första stycket 8 utlänningsdatalagen finns en hänvisning till 33–35 §§ PuL, som gäller överföring av personuppgifter till tredje land. Våra överväganden i denna del finns i kapitel 16.

### 9.4.8 Personuppgiftsombud och förhandskontroll

I 8 § första stycket 9 utlänningsdatalagen finns hänvisningar till 38–41 §§ PuL. Dessa bestämmelser reglerar vilka arbetsuppgifter ett personuppgiftsombud har samt en rätt för regeringen att meddela föreskrifter om att vissa behandlingar av personuppgifter ska anmälas för förhandskontroll till tillsynsmyndigheten.

I kapitel 11 redogör vi för vårt förslag om hur utlänningsdatalagens bestämmelser om personuppgiftsombud bör förändras med anledning av dataskyddsförordningen.

I artikel 55–58 i dataskyddsförordningen finns bestämmelser om tillsynsmyndigheternas behörighet, uppgifter och befogenheter. Här finns bl.a. – i artikel 36 samt 58.3 a och d – bestämmelser om förhandssamråd och förhandstillstånd, som är dataskyddsförordningens motsvarighet till personuppgiftslagens bestämmelser om förhandskontroll. Mot bakgrund av vårt tidigare ställningstagande anser vi att någon hänvisning till dataskyddsförordningens bestämmelser inte bör göras i denna del. Upplysningsvis kan sägas att möjligheten att med stöd av artikel 36.5 i dataskyddsförordningen införa nationella bestämmelser om krav på förhandstillstånd av tillsynsmyndigheten för vissa behandlingar, inte har utnyttjats i det förslag till dataskyddslag som finns i Dataskyddsutredningens betänkande (SOU 2017:39 s. 243 ff.).

### 9.4.9 Upplysningar till allmänheten om vissa behandlingar

Enligt huvudregeln i personuppgiftslagen (36 § första stycket) ska behandling av personuppgifter som är helt eller delvis automatiserad anmälas till tillsynsmyndigheten. Om den personuppgiftsansvarige har utsett ett personuppgiftsombud och anmält detta till tillsynsmyndigheten, görs dock undantag från skyldigheten att anmäla personuppgiftsbehandlingen (37 § PuL). Personuppgiftsombudet ska, enligt 39 § PuL, föra en förteckning över de behandlingar som den personuppgiftsansvarige genomför och som skulle ha omfattas av anmälningsskyldigheten i 36 § PuL om ombudet inte hade funnits.

I 8 § första stycket 10 utlänningsdatalagen finns en hänvisning till 42 § PuL. Av den sistnämnda bestämmelsen framgår i korthet att den personuppgiftsansvarige, till var och en som begär det, ska

lämna upplysningar om sådana automatiserade eller andra behandlingar av personuppgifter som inte har anmälts till tillsynsmyndigheten. Upplysningarna ska omfatta det som en anmälan till tillsynsmyndigheten enligt 36 § första stycket PuL skulle ha omfattat. Undantag görs för sekretessbelagda uppgifter eller uppgift om vilka säkerhetsåtgärder som har vidtagits.

Det finns ingen motsvarighet till 42 § PuL i dataskyddsförordningen. Enligt Dataskyddsutredningens förslag kommer inte heller dataskyddslagen att innehålla någon liknande bestämmelse.<sup>4</sup>

I detta sammanhang kan dock nämnas att det, när dataskyddsförordningen börjar tillämpas, kommer att vara den personuppgiftsansvarige som ska föra en förteckning över den personuppgiftsbehandling som utförs under dess ansvar. Detta framgår av artikel 30 i förordningen. Vi gör bedömningen att ett register som förs i enlighet med artikel 30 i förordningen måste anses vara upprättat i enlighet med 2 kap. 7 § TF; antingen som en färdigställd administrativ handling enligt första stycket eller som ett register enligt andra stycket 1. Allmänheten kommer därmed att ha rätt att få ut dess offentliga innehåll med stöd av tryckfrihetsförordningen. Vi gör därmed bedömningen att dataskyddsförordningen i praktiken inte kommer att innebära någon större förändring vad gäller allmänhetens tillgång till information om myndigheters personuppgiftsbehandling.

#### 9.4.10 Tillsynsmyndighetens handläggning och beslut

**Förslag:** Dataskyddslagens bestämmelser om tillsynsmyndighetens handläggning och beslut ska gälla även på utlänningsdatalagens tillämpningsområde. Regleringen ska genomföras genom en hänvisning i utlänningsdatalagen till de föreslagna bestämmelserna i 6 kap. 1–5 §§ dataskyddslagen.

I 8 § första stycket 11 utlänningsdatalagen finns hänvisningar till 43 och 44 §§, 45 § första stycket och 47 § PuL. Här regleras

---

<sup>4</sup> Se Dataskyddsutredningens betänkande (SOU 2017:39).

tillsynsmyndighetens befogenheter att vidta åtgärder mot de personuppgiftsansvariga.

Tillsynsmyndighetens behörighet, uppgifter och befogenheter regleras utförligt i artikel 55–59 i dataskyddsförordningen. Enligt dessa bestämmelser har tillsynsmyndigheten bl.a. befogenhet att behandla klagomål från registrerade, utfärda varningar och reprimander mot personuppgiftsansvariga, rikta förelägganden mot personuppgiftsansvariga samt besluta om begränsning av eller förbud mot en viss behandling. Tillsynsmyndigheten har enligt artikel 83 i dataskyddsförordningen även rätt att påföra de personuppgiftsansvariga administrativa sanktionsavgifter. Våra överväganden vad gäller sanktionsavgifter finns i avsnitt 9.4.14. Mot bakgrund av vårt tidigare ställningstagande anser vi att någon hänvisning till dataskyddsförordningens bestämmelser om tillsynsmyndighetens befogenheter m.m. inte bör göras.

Enligt det förslag som finns i Dataskyddsutredningens betänkande (SOU 2017:39) kommer dataskyddslagen dock att innehålla vissa kompletterande bestämmelser om tillsynsmyndighetens handläggning och beslut. Dessa finns enligt förslaget i 6 kap. dataskyddslagen. I de följande avsnitten kommer vi att redogöra för dessa bestämmelser och för varje bestämmelse göra en bedömning av om den bör gälla även på utlänningsdatalagens tillämpningsområde.

## Tillsynsmyndighetens befogenheter

Av förslaget till 6 kap. 1 § dataskyddslagen framgår att de befogenheter som tillsynsmyndigheten har enligt artikel 58.1–3 i dataskyddsförordningen ska gälla även vid tillsyn över efterlevnaden av bestämmelserna i dataskyddslagen och andra författningar som kompletterar dataskyddsförordningen. De aktuella bestämmelserna i dataskyddsförordningen handlar om tillsynsmyndighetens utredningsbefogenheter, korrigerande befogenheter och befogenheter att utfärda tillstånd och ge råd.

Som framgår av ordalydelsen i 6 kap. 1 § dataskyddslagen ska tillsynsmyndighetens befogenheter gälla oavsett om de kompletterande nationella bestämmelserna finns i dataskyddslagen eller i sektorsspecifika registerförfattningar. Dataskydds-

utredningen uttalar i sitt betänkande (SOU 2017:39 s. 311) att det krävs att tillsynsmyndigheten kan vidta samma åtgärder vid sin tillsyn över efterlevnaden av de nationella bestämmelser som kompletterar förordningen, för att dataskyddsförordningens intentioner ska få genomslag.

Det finns enligt vår mening inte några bärande skäl mot att tillsynen över den personuppgiftsbehandling som sker inom utlänningsdatalagens tillämpningsområde sker på samma sätt som för övriga myndigheter. Mot den bakgrunden föreslår vi att det tas in en hänvisning till 6 kap. 1 § dataskyddslagen i utlänningsdatalagen. På detta sätt kommer dataskyddsförordningens bestämmelser om tillsynsmyndighetens utredningsbefogenheter, korrigerande befogenheter samt befogenheter att utfärda tillstånd och ge råd, att gälla även för den tillsyn som sker över myndigheternas tillämpning av dataskyddslagens (i tillämpliga delar) och utlänningsdatalagens bestämmelser.

### **Ansökan hos förvaltningsrätten**

Enligt förslaget till 6 kap. 2 § första stycket dataskyddslagen gäller följande. 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. Artikel 58.2 i förordningen reglerar tillsynsmyndighetens korrigerande befogenheter, så som att förelägga en personuppgiftsansvarig att radera personuppgifter eller att förbjuda en personuppgiftsansvarig att behandla personuppgifter.

Enligt förslaget framgår det av 6 kap. 2 § andra stycket dataskyddslagen att tillsynsmyndighetens ansökan i dessa fall ska göras hos den förvaltningsrätt som är behörig att pröva ett överklagande av tillsynsmyndighetens beslut. I den föreslagna 8 kap. 6 § dataskyddslagen klargörs att denna typ av beslut kan överklagas (se avsnitt 19.4) och av 6 kap. 2 § tredje stycket dataskyddslagen framgår att det krävs prövningstillstånd vid överklagande till kammarrätten.

Dataskyddsutredningen redogör i sitt betänkande (SOU 2017:39 s. 318 f.) för innebörden av 6 kap. 2 § dataskyddslagen på följande sätt.

Om det finns skäl att ifrågasätta om en unionsrättsakt som påverkar tillämpningen av dataskyddsförordningen är giltig, till exempel om ett kommissionsbeslut 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./.../ 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.

De situationer som bestämmelsen i 6 kap. 2 § dataskyddslagen avser att träffa bör rimligen vara sällsynt förekommande. Enligt vår mening finns det dock inte anledning att ha en annan reglering för den tillsyn som sker på utlänningsdatalagens tillämpningsområde. Det bör därför enligt vår mening införas en hänvisning i utlänningsdatalagen till 6 kap. 2 § dataskyddslagen.

### **Kommunicering och delgivning**

Av den föreslagna 6 kap. 3 § dataskyddslagen framgår att innan tillsynsmyndigheten fattar ett beslut enligt artikel 58.2 i dataskyddsförordningen (se under föregående rubrik), ska den som beslutet gäller ges tillfälle att inom en bestämd tid yttra sig över allt material av betydelse för beslutet. Undantag görs om det är uppenbart obehövligt. Om saken är brådskande får tillsynsmyndigheten dock, 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.

Enligt den föreslagna 6 kap. 4 § dataskyddslagen ska ett beslut enligt 6 kap. 3 § delges, om det inte är uppenbart obehövligt. Delgivning enligt 34–37 §§ delgivningslagen (2010:1932) får användas bara om det finns särskild anledning att anta att mottagaren har avvikit eller på annat sätt håller sig undan. Paragraferna i delgivningslagen avser vissa typer av stämmningsmannadelgivning, som innebär att handlingen överlämnas till en annan person än delgivningsmottagaren.

Bestämmelser om kommunicering och delgivning finns i 46 § PuL, som gäller i samband med att tillsynsmyndigheten beslutar om vite. Dessa bestämmelser motsvarar de föreslagna bestämmelserna i 6 kap. 3 och 4 §§ dataskyddslagen. Personuppgiftslagens bestämmelser om vite gäller inte på utlänningsdatalagens tillämpningsområde (se 8 § tredje stycket utlänningsdatalagen) och det har därmed inte funnits någon anledning att ta in en hänvisning till 46 § PuL i utlänningsdatalagen.

Enligt artikel 83.5 e och 85.6 i dataskyddsförordningen ska den personuppgiftsansvarige påföras administrativa sanktionsavgifter om denne inte rättar sig efter ett föreläggande som meddelats av tillsynsmyndigheten. Detta innebär att de administrativa sanktionsavgifterna i vissa delar får samma effekt som ett vite. Mot bakgrund av att underlåtenheten att följa ett föreläggande kan leda till att administrativa sanktionsavgifter tas ut har Dataskyddsutredningen gjort bedömningen att de processuella skyddsåtgärder som nu kringgärdar tillsynsmyndighetens vitesförelägganden bör gälla för alla beslut som myndigheten kan meddela med stöd av artikel 58.2 i dataskyddsförordningen. Mottagaren av tillsynsmyndighetens föreläggande bör därmed som huvudregel, precis som enligt 46 § PuL, både få möjlighet att yttra sig över materialet i ärendet och få del av föreläggandet på något av de sätt som föreskrivs i delgivningslagen (se SOU 2017:39 s. 313 f.).

Administrativa sanktionsavgifter ska enligt vårt förslag få riktas även mot de myndigheter som behandlar personuppgifter inom utlänningsdatalagens tillämpningsområde (se avsnitt 9.4.14). För det fall tillsynsmyndigheten beslutar om ett föreläggande gentemot någon av de myndigheter som omfattas av utlänningsdatalagen finns det enligt vår mening inte anledning att ha ett annat förfarande än det som kommer att gälla för andra myndigheter. Vi anser därför att en hänvisning till 6 kap. 3 och 4 §§ dataskyddslagen

bör tas in i utlänningsdatalagen. Det faktum att de typer av stämmningsmannadelgivning som regleras i 34–37 §§ delgivningslagen inte kommer att bli aktuella för dessa myndigheter föranleder enligt vår mening inte i sig någon särreglering.

### **Besked angående handläggningen av ett klagomål**

Av den föreslagna 6 kap. 5 § dataskyddslagen framgår att 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. Sådant besked eller beslut ska meddelas inom två veckor från den dag då begäran om besked kom in till tillsynsmyndigheten. Om tillsynsmyndigheten har avslagit en begäran om besked, får den registrerade ge in en ny begäran om besked i ärendet tidigast tre månader efter det att myndighetens beslut meddelades.

Av Dataskyddsutredningens betänkande (SOU 2017:39 s. 305 ff.) framgår att förslaget till 6 kap. 5 § dataskyddslagen har införts för att uppfylla det krav på effektivt rättsmedel som garanteras genom dataskyddsförordningen. Som vi framfört i tidigare avsnitt anser vi att det inte finns anledning att ha ett annat förfarande för den tillsyn som sker på utlänningsdatalagens tillämpningsområde än det som kommer att gälla vid tillsyn över andra myndigheter. Vi anser därför att en hänvisning till 6 kap. 5 § dataskyddslagen bör tas in i utlänningsdatalagen.

#### **9.4.11 Skadestånd**

I 8 § första stycket 12 utlänningsdatalagen finns hänvisningar till 48 § PuL, som gäller den registrerades rätt till skadestånd. I avsnitt 14.8 finns en redogörelse för vad som kommer att gälla i denna fråga när dataskyddsförordningen börjar tillämpas. Där finns även våra överväganden av vilka hänvisningar som ska göras till dataskyddslagen i denna del.



### 9.4.12 Överklagande

I 8 § första stycket 13 utlänningsdatalagen finns en hänvisning till 51 §, 52 § första stycket och 53 § PuL, som reglerar rätten att överklaga beslut. Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) föreslagit nya, generellt tillämpliga, överklagandebestämmelser i dataskyddslagen. I avsnitt 19.4 finns våra överväganden kring vilka hänvisningar som bör göras till dataskyddslagen i denna del.

### 9.4.13 Förhållandet till tryck- och yttrandefriheten

**Förslag:** Bestämmelserna i dataskyddsförordningen, utlänningsdatalagen och dataskyddslagen ska inte tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Regleringen ska genomföras genom en hänvisning i utlänningsdatalagen till den föreslagna bestämmelsen i 1 kap. 4 § dataskyddslagen.

Av artikel 85.1 i dataskyddsförordningen följer att medlemsstaterna i lag ska förena rätten till integritet i enlighet med förordningen med bl.a. yttrande- och informationsfriheten. Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) föreslagit att det av 1 kap. 4 § första stycket dataskyddslagen ska framgå att bestämmelserna i den lagen och i dataskyddsförordningen inte ska tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Bestämmelsen motsvarar den reglering som för närvarande finns i 7 § första stycket PuL, som innebär att bestämmelserna i personuppgiftslagen inte ska tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Det finns för närvarande inte någon hänvisning i utlänningsdatalagen till den sistnämnda bestämmelsen.

Dataskyddsutredningen har föreslagit att dataskyddslagen ska vara subsidiär till bestämmelser som rör behandling av personuppgifter i annan lag eller författning (1 kap. 3 § dataskyddslagen).

Denna reglering innebär att tryckfrihetsförordningen gäller före dataskyddslagen, något som dessutom följer redan av allmänna rättsliga principer om att bestämmelser i vanlig lag inte tar över bestämmelser i grundlag (lex superior). Hur tryck- och yttrandefrihetsgrundlagarnas bestämmelser förhåller sig till dataskyddsförordningens bestämmelser är emellertid inte lika självklart. Mot den bakgrunden föreslår vi att det i utlänningsdatalagen görs en hänvisning till den föreslagna 1 kap. 4 § första stycket dataskyddslagen. Hänvisningen ska förstås så att även utlänningsdatalagens bestämmelser får ge vika för bestämmelserna om tryck- och yttrandefrihet. Bestämmelsens andra stycke, som gäller personuppgifter som behandlas för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande är enligt vår mening inte relevanta för verksamhet inom utlänningsdatalagens tillämpningsområde.

#### 9.4.14 Sanktionsavgifter

**Förslag:** Dataskyddslagens bestämmelser om administrativa sanktionsavgifter ska, med undantag för den bestämmelse som gäller överträdelse mot artikel 10 i dataskyddsförordningen, gälla även på utlänningsdatalagens tillämpningsområde. Regleringen ska genomföras genom en hänvisning i utlänningsdatalagen till de föreslagna bestämmelserna i 7 kap. 1, 3 och 4 §§ dataskyddslagen.

Enligt artikel 83 i dataskyddsförordningen har tillsynsmyndigheten i vissa fall möjlighet att påföra de personuppgiftsansvariga administrativa sanktionsavgifter vid överträdelse av förordningens bestämmelser. Av artikel 83.7 framgår att varje medlemsstat får fastställa regler för om och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter och organ som är inrättade i medlemsstaten.

Dataskyddsutredningen föreslår i sitt betänkande (SOU 2017:39) att 7 kap. 1–4 §§ dataskyddslagen ska innehålla bestämmelser om administrativa sanktionsavgifter. Enligt den föreslagna 7 kap. 1 § första stycket dataskyddslagen får sanktionsavgifter tas ut även av myndigheter vid överträdelse som avses i

artikel 83.4–6 i dataskyddsförordningen, varvid artikel 83.1–3 i förordningen ska tillämpas. De sistnämnda leden reglerar principerna för påförande av sanktionsavgifter. Enligt den föreslagna 7 kap. 1 § andra stycket dataskyddslagen ska avgiften bestämmas till högst 10 000 000 kr vid överträdelser som avses i artikel 83.4 i dataskyddsförordningen och annars till högst 20 000 000 kr.

I den föreslagna 7 kap. 2 § dataskyddslagen anges att sanktionsavgift får tas ut vid överträdelser av artikel 10 i dataskyddsförordningen. Bestämmelsen reglerar även avgiftens storlek i sådana fall. Administrativa sanktionsavgifter får vidare, enligt den föreslagna 7 kap. 3 § dataskyddslagen, inte beslutas om den som avgiften ska tas ut av inte har fått tillfälle att yttra sig enligt 6 kap. 3 § dataskyddslagen inom fem år från den dag då överträdelsen ägde rum (se avsnitt 9.4.10 under rubriken Kommunicering och delgivning). Enligt 7 kap. 4 § dataskyddslagen ska sanktionsavgifter som beslutats enligt dataskyddsförordningen eller dataskyddslagen tillfalla staten.

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39 s. 288 ff.) gjort bedömningen att övervägande skäl talar för att administrativa sanktionsavgifter ska kunna påföras statliga och kommunala myndigheter. Som grund för bedömningen framhöll Dataskyddsutredningen bl.a. den omfattning av känsliga personuppgifter som hanteras av myndigheter, att enskildas intresse av skydd för den personliga integriteten väger lika tungt vid behandling av personuppgifter i det allmännas verksamhet som i den privata sektorn och att behovet av avskräckande sanktioner inte är mindre när det gäller myndigheternas personuppgiftsbehandling.

För den personuppgiftsbehandling som utförs inom utlänningsdatalagens tillämpningsområde anser vi även i detta fall att det inte finns anledning att ha ett annat förfarande för tillsyn än det som kommer att gälla för andra myndigheter (jfr avsnitt 9.4.10). Vi anser därför att en hänvisning till 7 kap. 1, 3 och 4 §§ dataskyddslagen bör tas in i utlänningsdatalagen.

Bestämmelsen i 7 kap. 2 § dataskyddslagen behandlar överträdelser av artikel 10 i dataskyddsförordningen, enligt vilken behandling av personuppgifter som rör bl.a. fällande domar i brottmål endast får utföras under kontroll av myndighet. Eftersom

myndigheter således inte kan göra sig skyldiga till överträdelser av artikel 10 i dataskyddsförordningen bör det enligt vår mening inte göras någon hänvisning till 7 kap. 2 § dataskyddslagen.

Dataskyddslagens föreslagna bestämmelser om sanktionsavgifter gäller endast överträdelser av de bestämmelser i dataskyddsförordningen som anges i artikel 83.4–6 i förordningen. Vad gäller nationella bestämmelser anges i artikel 83.5 d att endast sådana bestämmelser som antagits enligt kapitel IX i förordningen kan föranleda sanktionsavgifter. Det gäller bland annat rätten att behandla uppgifter om nationella identifikationsnummer (artikel 87) och rätten att behandla personuppgifter i anställningsförhållanden (artikel 88). Detta innebär enligt vår mening motsatsvis att överträdelser av andra nationella bestämmelser än sådana som införts med stöd av kapitel IX inte träffas av dataskyddsförordningens bestämmelser om sanktionsavgifter. Eventuellt skulle dock överträdelser av nationella bestämmelser som utgör ett förtydligande av dataskyddsförordningens bestämmelser kunna ses som en överträdelse av förordningens bestämmelser och därmed kunna föranleda sanktionsavgift.

Som vi anført ovan anser vi att tillsynsmyndigheten bör tillämpa samma förfarande vid tillsyn mot de myndigheter som omfattas av utlänningsdatalagens tillämpningsområde som mot andra myndigheter. Det finns enligt vår mening emellertid inte anledning att utöka tillsynsmyndighetens möjligheter att besluta om sanktionsavgifter för dessa myndigheter.

## 10 Personuppgiftsansvaret

**Bedömning:** Dataskyddsförordningen föranleder ingen ändring av utlänningsdatalagens bestämmelse om personuppgiftsansvaret.

I artikel 4.7 i dataskyddsförordningen definieras personuppgiftsansvarig som 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. Enligt samma artikel finns också en möjlighet att i nationell lagstiftning föreskriva vem som är personuppgiftsansvarig för en viss personuppgiftsbehandling. En förutsättning för detta är att ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt. Även i skäl 45 till dataskyddsförordningen framhålls att vem som är personuppgiftsansvarig kan fastställas i den nationella rätten.

Definitionen av personuppgiftsansvaret i dataskyddsförordningen innebär ingen förändring gentemot tidigare regelverk. Artikel 4.7 i dataskyddsförordningen motsvaras av artikel 2 d i 1995 års dataskyddsdirektiv.

Inom utlänningsdatalagens tillämpningsområde har den svenska lagstiftaren utnyttjat möjligheten att i nationell registerlagstiftning peka ut vem som är personuppgiftsansvarig. Enligt 9 § utlänningsdatalagen är Migrationsverket, Polismyndigheten och en utlandsmyndighet var och en personuppgiftsansvariga för den behandling av personuppgifter som myndigheten utför. Migrationsverket är dock personuppgiftsansvarigt för utlandsmyndigheternas automatiserade behandling av personuppgifter.

I förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 55–56) görs följande bedömning. Huvudregeln bör vara att den som

utför själva behandlingen också har personuppgiftsansvaret. Således bör Migrationsverket och Polismyndigheten även fortsättningsvis vara personuppgiftsansvariga för den behandling som respektive myndighet utför. När det gäller den personuppgiftsbehandling som sker vid utlandsmyndigheterna finns det skäl som talar både för och emot att Migrationsverket ska vara personuppgiftsansvarigt för denna behandling. Regeringen anser dock att det tyngsta argumentet för detta är att verket redan tidigare hade detta ansvar och att denna ordning bedöms ha fungerat tillfredsställande.<sup>1</sup> Anledningen till att verkets personuppgiftsansvar har begränsats till utlandsmyndigheternas automatiserade behandling är att det är denna behandling som Migrationsverket har möjlighet att utöva kontroll över.

Frågan om personuppgiftsansvaret för den personuppgiftsbehandling som utförs inom utlänningsdatalagens tillämpningsområde har således behandlats genom överväganden i tidigare förarbeten. Dataskyddsförordningen föranleder inte någon ändring av den rådande ordningen, eftersom möjligheten att i bl.a. registerförfattning utpeka vem som är personuppgiftsansvarig kvarstår. Vi föreslår därför inte någon ändring av utlänningsdatalagen i denna del.

---

<sup>1</sup> Se 2 § första stycket förordningen (2001:720) om behandling av personuppgifter i verksamhet enligt utlännings- och medborgarskapslagstiftningen.

# 11 Dataskyddsbud

## 11.1 1995 års dataskyddsdirektiv, personuppgifts-lagen och utlänningsdatalagen

I artikel 18.2 i 1995 års dataskyddsdirektiv finns bestämmelserna om det nuvarande personuppgiftsombudets (i direktivet benämnt uppgiftsskyddsombudets) arbetsuppgifter. För det fall ett personuppgiftsombud utses får medlemsstaterna föreskriva att automatiserade behandlingar inte behöver anmälas till tillsynsmyndigheten. Enligt bestämmelsen ska ett personuppgiftsombud på ett oberoende sätt säkerställa den interna tillämpningen av de nationella bestämmelser som antagits till följd av direktivet. Ombudet ska också föra ett register över de behandlingar som utförs av den registeransvarige. Syftet är att säkerställa att de registrerades fri- och rättigheter sannolikt inte kommer att kränkas som en följd av personuppgiftsbehandling. Enligt artikel 20.2 i 1995 års dataskyddsdirektiv kan personuppgiftsombudet även göra en anmälan till tillsynsmyndigheten om förhandskontroll av personuppgiftsbehandlingar som kan innebära särskilda risker.

Enligt 10 § första stycket utlänningsdatalagen ska Migrationsverket och Polismyndigheten var och en utse ett eller flera personuppgiftsombud. För utlandsmyndigheterna är det för närvarande frivilligt att avgöra om de vill ha ett personuppgiftsombud eller inte.<sup>1</sup> Av 10 § andra stycket utlänningsdatalagen framgår att den personuppgiftsansvarige ska anmäla till tillsynsmyndigheten när ett personuppgiftsombud utses eller entledigas.

De bestämmelser i 1995 års dataskyddsdirektiv som gäller personuppgiftsombud har genomförts i svensk rätt genom 38–40 §§ PuL.

---

<sup>1</sup> Se förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 57).

Utlänningsdatalagen hänvisar, i 8 § första stycket 9, till dessa bestämmelser.

Enligt 38 § PuL gäller följande. Personuppgiftsombudet ska ha till uppgift att självständigt se till att den personuppgiftsansvarige behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed. Ombudet ska också påpeka eventuella brister för den personuppgiftsansvarige. Med personuppgiftsombudets ansvar följer enligt personuppgiftslagen även en skyldighet att göra en anmälan till tillsynsmyndigheten om ombudet har anledning att misstänka att den personuppgiftsansvarige bryter mot de bestämmelser som gäller för behandlingen av personuppgifter och inte vidtar rättelse efter påpekande. Även i övrigt ska personuppgiftsombudet samråda med tillsynsmyndigheten vid tveksamhet om hur de bestämmelser som gäller för behandlingen av personuppgifter ska tillämpas.

Personuppgiftsombudet ska, enligt 39 § PuL, föra en förteckning över vissa av de behandlingar som den personuppgiftsansvarige genomför och som skulle ha omfattats av anmälningskyldighet till tillsynsmyndigheten om ombudet inte hade funnits.

Slutligen ska personuppgiftsombudet, enligt 40 § PuL, hjälpa registrerade att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga.

## 11.2 Dataskyddsförordningen

### 11.2.1 Myndigheter ska utse dataskyddsbud

Enligt artikel 37.1 a i dataskyddsförordningen ska myndigheter som utför personuppgiftsbehandling ”under alla omständigheter” utse ett dataskyddsbud.<sup>2</sup> Termen dataskyddsbud definieras inte i förordningen. I artikel 37–39 i förordningen beskrivs dock bl.a. dataskyddsbudets uppgifter och förhållande till den personuppgiftsansvarige. Utifrån dessa bestämmelser kan man dra slutsatsen att dataskyddsbudet motsvarar det som i 1995 års dataskyddsdirektiv benämns uppgiftsskyddsbud och som i personuppgiftslagen kallas personuppgiftsombud.

---

<sup>2</sup> Endast den personuppgiftsbehandling som sker som en del av domstolarnas dömande verksamhet är undantagen från denna skyldighet.



### 11.2.2 Dataskyddsbudets ställning, uppgifter m.m.

Dataskyddsbudet beskrivs i skäl 97 till dataskyddsförordningen som "en person med sakkunskap i fråga om dataskyddslagstiftning och -förfaranden". Artikel 37 i förordningen innehåller diverse bestämmelser om dataskyddsbudet. Ombudet ska utses på grundval av yrkesmässiga kvalifikationer och bl.a. ha sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som förordningen ålägger ett dataskyddsbud (37.5). Det anges vidare att dataskyddsbudet antingen kan vara en anställd eller utföra uppgiften på grund av tjänsteavtal (37.6). Dataskyddsbudets kontaktuppgifter ska offentliggöras och meddelas till tillsynsmyndigheten (37.7). Vidare framgår att ett enda dataskyddsbud får utnämnas för flera personuppgiftsansvariga myndigheter, med hänsyn till organisationsstruktur och storlek (37.3). Det finns ingen ledning i dataskyddsförordningens skäl om hur bestämmelsen om gemensamt dataskyddsbud ska tolkas. Det man kan sluta sig till är enligt vår mening endast det som framgår av bestämmelsen; de myndigheter som vill utse ett gemensamt dataskyddsbud måste göra en bedömning av om detta är lämpligt utifrån samtliga inblandade myndigheters organisationsstruktur och storlek.

I artikel 38 redogörs bl.a. för dataskyddsbudets självständiga ställning gentemot den personuppgiftsansvarige. Som exempel kan nämnas följande. Den personuppgiftsansvarige ska se till att dataskyddsbudet har tillgång till de uppgifter och resurser som krävs för att fullgöra uppdraget och upprätthålla sin sakkunskap (38.2). Vidare ska den personuppgiftsansvarige säkerställa att ombudet inte tar emot instruktioner om hur han eller hon ska utföra sina uppgifter. Ombudet får inte heller avsättas eller bli föremål för sanktioner för att ha utfört sina uppgifter (38.3). Dataskyddsbudet får fullgöra andra uppgifter och uppdrag, men den personuppgiftsansvarige ska se till att dessa inte leder till en intressekonflikt (38.6).

Av artikel 38.5 i dataskyddsförordningen framgår att dataskyddsbudet vid genomförande av sina uppgifter ska vara bundet av sekretess eller konfidentialitet i enlighet med unionsrätten eller medlemsstaternas nationella rätt. Mot den bakgrunden har Dataskyddsutredningen i sitt betänkande (SOU 2017:39)

föreslagit att det i 1 kap. 6 § första stycket dataskyddslagen ska regleras att den som fullgör uppgift som dataskyddsombud inte obehörigen får röja eller utnyttja det som han eller hon då har fått veta om enskilds personliga och ekonomiska förhållanden. Enligt andra stycket i samma bestämmelse ska det enligt utredningens förslag framgå att offentlighets- och sekretesslagen tillämpas i det allmännas verksamhet i stället för första stycket.

Enligt 2 kap. 1 § första stycket OSL är det förbjudet för myndigheter att röja eller utnyttja en uppgift som det råder sekretess för. Det samma gäller enligt andra stycket för personer som fått kännedom om uppgiften genom att han eller hon för det allmännas räkning deltagit i en myndighets verksamhet på grund av anställning eller uppdrag hos myndigheten, på grund av tjänsteplikt eller på annan liknande grund. Dataskyddsutredningen har gjort bedömningen att en myndighets dataskyddsombud i allmänhet får anses delta i verksamheten på ett sådant sätt som avses i 2 kap. 1 § andra stycket OSL och att han eller hon därmed omfattas av den sekretess som gäller för den aktuella myndigheten.<sup>3</sup>

Artikel 39.1 i dataskyddsförordningen reglerar dataskyddsombudets uppgifter. Dessa ska enligt bestämmelsen åtminstone vara följande.

- a) Informera och ge råd till den personuppgiftsansvarige, personuppgiftsbiträdet och de anställda om deras skyldigheter enligt dataskyddsförordningen och andra dataskyddsbestämmelser.
- b) Övervaka efterlevnaden av dataskyddsförordningen och andra dataskyddsbestämmelser samt efterlevnaden av den personuppgiftsansvariges eller personuppgiftsbitrådets strategi för skydd av personuppgifter. Detta inbegriper ansvarstildelning, information till och utbildning av personal.
- c) På begäran ge råd vad gäller sådana konsekvensbedömningar avseende dataskydd som enligt artikel 35 ska göras om en typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Dataskyddsombudet ska också övervaka genomförandet av en sådan konsekvensbedömning.
- d) Samarbete med tillsynsmyndigheten.

---

<sup>3</sup> Se Dataskyddsutredningens betänkande (SOU 2017:39 s. 262).

- e) Vara kontaktpunkt för tillsynsmyndigheten i frågor som rör personuppgiftsbehandling. I detta ingår det förhandssamråd som enligt artikel 36 ska genomföras med tillsynsmyndigheten om en konsekvensbedömning enligt artikel 35 visar att behandlingen utan vidtagna åtgärder leder till en hög risk. Vid behov ska samråd även ske i alla andra frågor.

Därtill får den registrerade, enligt artikel 38.4 i dataskyddsförordningen, kontakta dataskyddsbudet när det gäller alla frågor som rör behandlingen av dennes personuppgifter och utövandet av dennes rättigheter enligt förordningen.

## 11.3 Bedömning

**Förslag:** Utlänningsdatalagens bestämmelser om personuppgiftsombud ska upphävas.

**Bedömning:** Någon hänvisning till dataskyddsförordningens bestämmelser om dataskyddsbud bör inte göras i utlänningsdatalagen.

### 11.3.1 Dataskyddsbudet – ”internrevisor” med något utökat uppdrag

Dataskyddsförordningens reglering är mer utförlig än 1995 års dataskyddsdirektivs och personuppgiftslagens reglering vad gäller dataskyddsbudets kvalifikationer och arbetsuppgifter. Även förhållandet till den personuppgiftsansvarige och dennes skyldigheter gentemot ombudet beskrivs mer detaljerat i förordningen. Frågan är emellertid om detta innebär någon skillnad i sak vad gäller de uppgifter ett dataskyddsbud förväntas utföra.

Enligt personuppgiftslagen ska personuppgiftsombudet se till att den personuppgiftsansvarige behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed. Han eller hon ska också påpeka eventuella brister i behandlingen för den personuppgiftsansvarige. Personuppgiftslagens beskrivning av ombudets arbetsuppgifter är således inte speciellt konkret, vilket naturligtvis öppnar för tolkningar av vad ombudet egentligen ska göra och hur

detta ska gå till. Vi kan dock inte se annat än att det i uppgiften att ”se till att personuppgifter behandlas lagligt och korrekt” samt ”påpeka eventuella brister för den personuppgiftsansvarige” bör ingå många av de uppgifter som ett dataskyddsbud uttryckligen åläggs enligt dataskyddsförordningen. Som exempel kan nämnas att informera och ge råd till både den personuppgiftsansvarige och de anställda gällande dataskyddsbestämmelser, att övervaka hur dessa bestämmelser följs och att medverka i arbetet kring konsekvensbedömningar avseende dataskydd.

Vidare bör en person som ska övervaka personuppgiftsbehandlingen på det sätt som beskrivs i personuppgiftslagen enligt vår mening ha de kvalifikationer (t.ex. sakkunskap inom rättsområdet) som beskrivs i dataskyddsförordningen för att klara av att genomföra uppdraget på ett tillfredsställande sätt.

I personuppgiftslagen föreskrivs att ombudet ska samråda med tillsynsmyndigheten vid tveksamheter. I dataskyddsförordningen föreskrivs i stället att ombudet ska samråda och samarbeta med tillsynsmyndigheten och vara dess kontaktpunkt. Detta innebär eventuellt att ombudets arbetsuppgifter utökas något genom dataskyddsförordningen. Enligt vår uppfattning lär det utökade ansvaret i sådant fall i huvudsak aktualiseras om Datainspektionen söker kontakt med antingen ombudet eller den personuppgiftsansvarige.

Av personuppgiftslagen framgår att personuppgiftsbudet självständigt ska utföra sina uppgifter. Dataskyddsförordningen är mycket mer detaljerad i denna del, främst vad gäller den personuppgiftsansvariges skyldigheter gentemot ombudet. Den personuppgiftsansvarige ska t.ex. se till att ombudet får tillräckliga resurser och inte tar emot instruktioner samt se till att det inte uppstår intressekonflikter med andra uppdrag. Som vi ser det förtydligar dataskyddsförordningens bestämmelser i denna del att det är den personuppgiftsansvarige som ska se till att ombudets självständighet upprätthålls. Vidare specificeras vad som utmärker ett självständigt ombud. Många av de krav som ställs på den personuppgiftsansvarige i denna del ter sig enligt vår mening dock som relativt självklara åtgärder för att upprätthålla ombudets självständighet.

Vissa av de uppgifter personuppgiftsbudet haft enligt personuppgiftslagen försvinner när dataskyddsförordningen börjar

tillämpas. Dataskyddsbudet kommer inte att ha skyldighet att göra en anmälan till tillsynsmyndigheten vid misstanke om att den personuppgiftsansvarige bryter mot dataskyddsbestämmelserna. Inte heller kommer ombudet längre att vara skyldigt att föra en förteckning över vissa av den personuppgiftsansvariges behandlingar. Denna skyldighet kommer i stället att, enligt artikel 30 i dataskyddsförordningen, åligga den personuppgiftsansvarige.

Slutligen beskrivs dataskyddsbudets skyldighet gentemot de registrerade på ett något annorlunda sätt i dataskyddsförordningen. Enligt personuppgiftslagen ska ombudet hjälpa de registrerade att få rättelse. Enligt dataskyddsförordningen (artikel 38.4) ”får den registrerade kontakta dataskyddsbudet” när det gäller frågor kring behandling av dennes personuppgifter eller rörande dennes rättigheter. Ordvalet gör att det kan diskuteras om dataskyddsbudets skyldigheter att vara de registrerade behjälpliga är lika långtgående som tidigare.

Med hänsyn till ovanstående gör vi bedömningen att dataskyddsbudets uppgifter enligt dataskyddsförordningen främst innebär ett uppdrag som ”internrevisor” för den personuppgiftsansvariges behandlingar. Uppdraget kan te sig något utökat jämfört med tidigare reglering. Beroende på hur uppdraget har utförts tidigare kan dataskyddsförordningen innebära vissa förändringar i ombudets uppgifter. Enligt vår bedömning bör det emellertid inte röra sig om några omfattande sådana. Det som främst kommer att orsaka merarbete jämfört med i dag är troligtvis i stället det faktum att det införs helt ny och relativt komplicerad lagstiftning på området.

### **11.3.2 Skyldigheten att utse dataskyddsbud och ombudets uppgifter framgår av dataskyddsförordningen**

Skyldigheten för myndigheter att utse ett dataskyddsbud kommer när dataskyddsförordningen börjar tillämpas att framgå direkt av förordningen. Förordningen ger förvisso en viss möjlighet att återge dess bestämmelser i nationell lagstiftning, t.ex. i syfte att göra de nationella bestämmelserna begripliga (se avsnitt 5.3). Enligt vår mening bör dock möjligheten att återge dataskyddsförordningens bestämmelser användas med försiktighet, eftersom det snarare kan skapa oklarheter för tillämparen om ett

återgivande görs av vissa bestämmelser men inte av andra. Vad gäller skyldigheten att utse dataskyddsbud är förordningens bestämmelse dessutom klar och tydlig till sin innebörd. Enligt vårt förslag kommer det vidare uttryckligen att framgå av utlänningsdatalagen att lagen innehåller kompletterande bestämmelser till dataskyddsförordningen. Mot den bakgrunden anser vi att förordningens bestämmelser om skyldigheten att utse dataskyddsbud inte bör tas in i utlänningsdatalagen. Vi föreslår därför att 10 § första stycket utlänningsdatalagen, som reglerar skyldigheten att utse personuppgiftsbud, ska utgå. I enlighet med den bedömning vi tidigare gjort (se bl.a. avsnitt 9.2) bör inte heller någon hänvisning till dataskyddsförordningens bestämmelser göras i denna del.

Enligt nuvarande 10 § andra stycket utlänningsdatalagen ska den personuppgiftsansvarige anmäla till tillsynsmyndigheten när ett personuppgiftsbud utses eller entledigas. Den personuppgiftsansvariges anmälningsskyldighet framgår dock redan av artikel 37.7 i dataskyddsförordningen. Bestämmelsen i utlänningsdatalagen bör enligt vår mening därför upphävas.

Även hänvisningen i 8 § 9 utlänningsdatalagen till 38–40 §§ PuL om personuppgiftsbud måste utgå. Personuppgiftslagen kommer att upphävas<sup>4</sup> och bestämmelser om dataskyddsbudets uppgifter finns i artikel 38.4 och artikel 39 i dataskyddsförordningen. Av de skäl som framgår ovan anser vi att det inte bör införas några hänvisningar till bestämmelserna i dataskyddsförordningen i denna del.

Det faktum att det – direkt med stöd av dataskyddsförordningen – kommer att vara obligatoriskt för myndigheter att utse ett dataskyddsbud innebär en förändring för utlandsmyndigheterna, som för närvarande själva får bedöma om ett personuppgiftsbud ska utses eller inte. Vi vill i detta sammanhang nämna möjligheten att enligt artikel 37.3 i dataskyddsförordningen utnämna ett gemensamt dataskyddsbud för flera myndigheter. Detta skulle kunna vara en lösning för de utlandsmyndigheter som anser att skyldigheten att utse ett dataskyddsbud blir betungande, exempelvis på grund av myndighetens storlek. Ett sådant beslut måste dock enligt vår

---

<sup>4</sup> Se kommittédirektiv till Dataskyddsutredningen (Dir 2016:15 s. 6).

mening föregås av en lämplighetsbedömning utifrån organisationsstruktur och myndigheternas storlek. Att göra en sådan bedömning ligger inte inom vårt uppdrag. Vi vill också påminna om att ett tjänsteavtal måste tecknas med ombudet om dataskyddsbudet inte är anställd inom den egna myndigheten (se artikel 37.6).

För stora myndigheter kan det finnas behov av att utse mer än ett dataskyddsbud. I dataskyddsförordningen benämns dataskyddsbudet emellertid endast som *ett* dataskyddsbud, dvs. i singular. Även i 1995 års dataskyddsdirektiv och personuppgiftslagen omnämns ombudet endast i singular, vilket inte har ansetts utgöra hinder mot att i utlänningsdatalagen och i andra myndigheters registerförfattningar föreskriva en möjlighet att utse flera ombud.<sup>5</sup> Syftet med dataskyddsförordningen är vidare att skydda fysiska personer när deras personuppgifter behandlas (artikel 1). Förekomsten av flera än ett dataskyddsbud i en stor organisation innebär en förstärkning av detta skydd och ligger således enligt vår mening i linje med dataskyddsförordningens intentioner. Mot den bakgrunden anser vi att det faktum att det i dataskyddsförordningen endast talas om *ett* ombud inte hindrar att flera ombud utses vid en och samma myndighet.

### 11.3.3 Tystnadsplikt för dataskyddsbudet

I dataskyddsförordningen förutsätts enligt vår bedömning att dataskyddsbudet är en fysisk person (jfr artikel 37.6 och skäl 97). Om uppdraget utförs av en anställd vid den personuppgiftsansvariga myndigheten kommer ombudet att omfattas av den tystnadsplikt som gäller för myndighetens anställda enligt offentlighets- och sekretesslagen.

Det finns emellertid inte något som hindrar att en myndighet anlitar en utomstående för uppdraget. Vi delar Dataskyddsutredningens bedömning att ett sådant dataskyddsbud får anses delta i myndighetens verksamhet på sådant sätt som avses i 2 kap. 1 § OSL och att ombudet därmed omfattas av den sekretess som gäller för personal vid myndigheten. En förutsättning för detta

---

<sup>5</sup> Se även 10 § domstolsdatalagen (2015:728), 2 kap. 5 § polisdatalagen (2010:361) och 2 kap. 4 § åklagardatalagen (2015:433).

torde dock vara att dataskyddsbudet är en särskilt förordnad och utpekad person, som med stöd av ett tjänsteavtal utför uppdraget. Vi anser att man bör kunna förutsätta att de aktuella myndigheterna uppfyller dessa krav om de anlitar en utomstående som dataskyddsbud. Mot den bakgrunden bedömer vi att det inte finns någon anledning att i utlänningsdatalagen införa en hänvisning till regleringen om tystnadsplikt för dataskyddsbud i den föreslagna 1 kap. 6 § dataskyddslagen.



## 12 Känsliga personuppgifter och sökbegränsningar

### 12.1 Känsliga personuppgifter

#### 12.1.1 Dataskyddsförordningen och 1995 års dataskyddsdirektiv

Behandling av känsliga personuppgifter regleras i artikel 9 i dataskyddsförordningen. Med känsliga personuppgifter menas enligt förordningen personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt uppgifter om hälsa, en persons sexualliv eller sexuella läggning. Även behandling av biometriska uppgifter för att entydigt identifiera en fysisk person och genetiska uppgifter utgör känsliga personuppgifter. Begreppet *känsliga personuppgifter* används inte uttryckligen i artikel 9, men förekommer i skäl 10 till dataskyddsförordningen. Det är också väl inarbetat i svensk rätt genom bl.a. 13 § PuL.

Begreppet *känsliga personuppgifter* har i dataskyddsförordningen utökats i förhållande till hur det såg ut i 1995 års dataskyddsdirektiv, genom att uppgifter om en persons sexuella läggning nu uttryckligen ingår i begreppet. Nytt är också att biometriska uppgifter för att entydigt identifiera en fysisk person och genetiska uppgifter utgör känsliga personuppgifter.

Enligt dataskyddsförordningens huvudregel, som framgår av artikel 9.1, är behandling av känsliga personuppgifter förbjuden. Det finns dock en rad undantag från detta förbud. Det undantag som främst är intressant för de myndigheter som tillämpar utlänningsdatalagen finns i artikel 9.2 g. Enligt denna bestämmelse är behandling av känsliga personuppgifter tillåten om den är nödvändig med hänsyn till ett viktigt allmänt intresse. Av

bestämmelsen framgår vidare att det ”viktiga allmänna intresset” ska framgå av unionsrätten eller av medlemsstaternas nationella rätt, som 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.

Även enligt 1995 års dataskyddsdirektiv är huvudregeln att behandling av känsliga personuppgifter är förbjuden. Något direkt undantag med hänsyn till viktiga allmänna intressen finns inte i direktivet. Enligt artikel 8.4 har medlemsstaterna dock möjlighet att med hänsyn till ett viktigt allmänt intresse besluta om ytterligare undantag från förbudet att behandla känsliga personuppgifter. Något generellt undantag som skulle kunna träffa den personuppgiftsbehandling som utförs inom utlänningsdatalagens tillämpningsområde har dock inte införts i personuppgiftslagen med stöd av artikel 8.4 i 1995 års dataskyddsdirektiv. Ett undantag för myndigheters behandling i löpande text av känsliga personuppgifter som lämnats i ett ärende eller är nödvändiga för handläggning av ett ärende har dock, med stöd av 20 § PuL, införts i 8 § personuppgiftsförordningen (1998:1191).

### 12.1.2 Dataskyddslagen

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) förslagit att dataskyddslagen ska innehålla bestämmelser om rätten att behandla känsliga personuppgifter. Enligt förslaget ska myndigheter få behandla känsliga personuppgifter i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det (3 kap. 3 § 1). Dataskyddsutredningen föreslår också att myndigheter ska få behandla känsliga personuppgifter om de lämnats till myndigheten och behandlingen krävs enligt annan lag (3 kap. 3 § 2). Anledningen till detta anges vara att det utgör ett viktigt allmänintresse att myndigheterna ska kunna sköta sitt uppdrag på ett korrekt, rättssäkert och effektivt sätt. Detta förutsätter att den grundlagsstadgade handlingsoffentligheten och andra lagstadgade skyldigheter upprätthålls. Det anges också att viss behandling av känsliga personuppgifter är

oundvikligt i myndigheternas verksamhet som en direkt följd av exempelvis tryckfrihetsförordningens, offentlighets- och sekretesslagens och förvaltningslagens bestämmelser. Sådan behandling bör uttryckligen tillåtas i dataskyddslagen så att det inte råder någon tveksamhet kring lagligheten av behandlingen.<sup>1</sup>

Utöver detta föreslår Dataskyddsutredningen att myndigheter i enstaka fall ska få behandla känsliga personuppgifter om det är absolut nödvändig för ändamålet med behandlingen och inte innebär ett otillbörligt intrång i den registrerades personliga integritet (3 kap. 3 § 3). En myndighet som behandlar känsliga personuppgifter enbart med stöd av 3 kap. 3 § dataskyddslagen ska enligt Dataskyddsutredningens förslag inte få använda sökbegrepp som avslöjar känsliga personuppgifter (3 kap. 4 §).

### 12.1.3 Utlänningsdatalagens allmänna bestämmelser

Känsliga personuppgifter förekommer i stor utsträckning i den verksamhet som bedrivs enligt utlännings- och medborgarskapslagstiftningen. I förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 79) bedömde regeringen att de undantag för behandling av känsliga personuppgifter som finns i personuppgiftslagen och personuppgiftsförordningen inte är tillräckliga för att täcka all nödvändig behandling av känsliga personuppgifter som utförs inom utlänningsdatalagens tillämpningsområde och att rätten att behandla känsliga personuppgifter därför borde regleras i den lagen.

Enligt 15 § första stycket 1 utlänningsdatalagen får sådana känsliga personuppgifter som anges i 13 § PuL endast behandlas för de ändamål som anges i 11 § 1–4 och 6 samt 13 § samma lag. Ytterligare en förutsättning för behandlingen är att uppgifterna ska vara absolut nödvändiga för syftet med behandlingen. Därutöver får, enligt 15 § första stycket 2 utlänningsdatalagen, känsliga personuppgifter behandlas i löpande text för det ändamål som anges i 12 § 2 (återsökning av information som rör förhållanden i andra länder) om uppgifterna är absolut nödvändiga för att fullgöra arbetsuppgifter i sådan verksamhet som faller under utlännings-

---

<sup>1</sup> Se Dataskyddsutredningens betänkande (SOU 2017:39 s. 176 f.).

datalagens tillämpningsområde.<sup>2</sup> Bestämmelsen i 15 § utlänningsdatalagen är uttömmande, vilket innebär att känsliga personuppgifter inte får behandlas i andra situationer än de uppräknade. Känsliga personuppgifter får således inte behandlas för utförande av testverksamhet (11 § 5 utlänningsdatalagen) eller för återsökning av avgöranden, rättsutredningar eller annan rättslig information (jfr 12 § 1 utlänningsdatalagen). Enligt 15 § andra stycket 1 utlänningsdatalagen har regeringen rätt att meddela ytterligare föreskrifter om inskränkningar av möjligheten att behandla känsliga personuppgifter. Några sådana bestämmelser finns inte i utlänningsdataförordningen.

#### **12.1.4 Migrationsverkets register över fingeravtryck och fotografier**

Av 14 § första stycket utlänningsdatalagen framgår att Migrationsverket får föra separata register över fingeravtryck och fotografier som tas med stöd av 9 kap. 8 § utlänningslagen (2005:716). Av bestämmelsens andra stycke följer att registrens uppgifter om fingeravtryck eller fotografier – med begränsning av de ändamål som annars gäller enligt 11 och 13 §§ – får användas endast i vissa utpekade verksamheter eller situationer. Dessa utgörs av prövning av vissa ansökningar om uppehållstillstånd (punkt 1), ärenden om avvísning eller utvisning (punkt 2), testverksamhet (punkt 3), för identitetskontroll i vissa fall (punkt 4) eller för kontroll av fingeravtryck mot Polismyndighetens fingeravtrycks- och signalementsregister (punkt 5).

Enligt 14 § tredje stycket utlänningsdatalagen får regeringen meddela ytterligare föreskrifter om vilka uppgifter som får behandlas i registren över fingeravtryck och fotografier samt föreskrifter om gallring. Av 2 § utlänningsdataförordningen framgår att register över fingeravtryck och fotografier endast får innehålla fingeravtryck och fotografier samt uppgifter om den registrerades namn, person- eller samordningsnummer, födelsetid, kön, medborgarskap eller annan identifieringsuppgift. I 3 § utlänningsdataförordningen finns föreskrifter om gallring av

---

<sup>2</sup> Tillämpningsområdet återfinns i 2 § utlänningsdatalagen, se avsnitt 7.2.1.

uppgifter i registren över fingeravtryck och fotografier. Denna bestämmelse behandlas i avsnitt 17.3.

### 12.1.5 Bedömning

**Förslag:** Utlänningsdatalagens definition av känsliga personuppgifter ska innehålla en hänvisning till artikel 9.1 i dataskyddsförordningen.

Personuppgifter i Migrationsverkets register över fingeravtryck och fotografier ska även fortsättningsvis få behandlas enligt de nuvarande förutsättningarna.

**Bedömning:** Dataskyddsförordningen innebär inte att det behövs någon nationell bestämmelse som ger rätt att behandla känsliga personuppgifter inom utlänningsdatalagens tillämpningsområde.

### Rätten att behandla känsliga personuppgifter

Vi bedömer att undantaget i artikel 9.2 g dataskyddsförordningen, som ger rätt att behandla känsliga personuppgifter om det är nödvändigt med hänsyn till ett viktigt allmänt intresse, omfattar all den verksamhet som bedrivs inom utlänningsdatalagens tillämpningsområde. Vi har i avsnitt 6.3.2 gjort bedömningen att denna verksamhet utgör en uppgift av allmänt intresse i dataskyddsförordningens mening. I personuppgiftslagen har undantaget som rör viktiga allmänna intressen (artikel 8.4 i 1995 års dataskyddsdirektiv) utnyttjats bl.a. för att införa regleringen i 19 § PuL om behandling av känsliga personuppgifter för forsknings- och statistikändamål. Med stöd av samma bestämmelse har medlemsstaterna infört undantag för behandling av känsliga personuppgifter i myndigheters verksamhet, på bankområdet och för att främja jämställdhet och social trygghet.<sup>3</sup> Att även de uppgifter av allmänt intresse som anförtrotts Migrationsverket,

<sup>3</sup> Artikel 29-gruppens Advice paper on special categories of data ("sensitive data"), beslutat den 20 april 2011.

Polismyndigheten och utlandsmyndigheterna på utlännings- och medborgarskapsområdet kan beskrivas som ”viktiga” anser vi mot den bakgrunden vara tämligen självklart.

Artikel 9.2 g i dataskyddsförordningen innehåller vissa krav som måste vara uppfyllda för att undantaget ska bli tillämpligt. För det första ska det viktiga allmänna intresset framgå av unionsrätten eller medlemsstaternas nationella rätt. För det andra ska denna lagstiftning 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.

Migrationsverkets, Polismyndighetens och utlandsmyndigheternas uppgifter på utlännings- och medborgarskapsområdet är fastställda genom författning. Vad gäller de grundläggande principerna för personuppgiftsbehandling motsvarar dataskyddsförordningen till allra största delen 1995 års dataskyddsdirektiv. Mot den bakgrunden anser vi att det får förutsättas att lagstiftaren bedömt att den behandling av personuppgifter som sker inom utlänningsdatalagens tillämpningsområde är proportionerlig mot syftet med behandlingen och inte oförenlig med det grundläggande skyddet för personuppgifter. Genom utlänningsdatalagen finns också bestämmelser som säkerställer skyddet för de registrerades integritet, t.ex. i form av behörighets- och sökbegränsningar.

Enligt utlänningsdatalagens sekundära ändamålsbestämmelse får personuppgifter behandlas för att tillhandahålla information till riksdagen eller regeringen eller till en annan myndighet eller enskild med stöd av lag eller förordning. Personuppgifter får också behandlas för att tillhandahålla information till en utländsk myndighet, ett EU-organ eller en mellanfolklig organisation om detta följer av uppgiftsskyldighet på grund av EU-medlemskapet, en internationell konvention eller riksdagens avtal med bl.a. främmande stat. Även känsliga personuppgifter kan naturligtvis ingå bland de personuppgifter som ska lämnas ut på dessa grunder.

Vi har, i avsnitt 6.3.2, gjort bedömningen att ett utlämnande av personuppgifter som sker i enlighet med lag eller förordning måste anses vara nödvändigt med hänsyn till ett allmänt intresse. Vi anser att detsamma bör gälla de utlämnanden som är nödvändiga för att tillhandahålla information till riksdag eller regering eller som följer

av Sveriges EU-medlemskap, en internationell konvention eller ett avtal som riksdagen godkänt. Undantaget i artikel 9.2 g i dataskyddsförordningen – viktigt allmänt intresse – är enligt vår mening därmed tillämpligt även för sådan behandling av känsliga personuppgifter som sker med stöd av utlänningsdatalagens sekundära ändamålsbestämmelse. Det får enligt vår mening vidare förutsättas att ett utlämnande av personuppgifter som föreskrivs i författning eller som är nödvändigt för något annat av de syften som framgår av utlänningsdatalagens sekundära ändamålsbestämmelse, är proportionerligt mot syftet med utlämnandet och inte oförenligt med det grundläggande skyddet för personuppgifter. För det fall utlämnandet av känsliga uppgifter sker till annan myndighet finns också ett skydd för uppgifterna, eftersom myndigheter enligt Dataskyddsutredningens förslag till dataskyddslag inte får använda sökbegrepp som avslöjar känsliga personuppgifter. Även de enskilda myndigheternas registerförfattningar kan, liksom utlänningsdatalagen, innehålla skyddsåtgärder i form av bl.a. sökbegränsningar eller behörighetsbegränsningar.

Sammanfattningsvis anser vi att samtliga de krav som ställs upp i artikel 9.2 g i dataskyddsförordningen för att känsliga personuppgifter ska få behandlas med hänsyn till ett viktigt allmänt intresse är uppfyllda för den personuppgiftsbehandling som sker inom ramen för utlänningsdatalagens primära och sekundära ändamålsbestämmelser. Dataskyddsförordningen tillåter enligt vår mening därmed att känsliga personuppgifter behandlas på hela utlänningsdatalagens tillämpningsområde om det är nödvändigt för att verksamheten ska kunna bedrivas. Någon nationell bestämmelse som ger rätt att behandla känsliga personuppgifter inom lagens tillämpningsområde behövs enligt vår mening därmed inte.

### **Begränsning av behandling av känsliga personuppgifter**

Som framgår av avsnitt 5.3 anser vi att det inte finns något hinder mot att medlemsstaterna inför mer restriktiva bestämmelser för sina myndigheters personuppgiftsbehandling än vad som följer av dataskyddsförordningen. Utlänningsdatalagens bestämmelser om hur känsliga personuppgifter får behandlas inom dess tillämpnings-

område kan därmed finnas kvar. Detsamma gäller bestämmelsen om behandling av personuppgifter i Migrationsverkets register över fingeravtryck och fotografier. Vi gör vidare, i avsnitt 18.2, bedömningen att dataskyddsförordningen inte hindrar att nationella bestämmelser om personuppgiftsbehandling införs i en förordning eller i en myndighetsföreskrift, så länge föreskrifterna tillkommit i laga ordning. Det behövs därmed inte heller i det avseendet någon förändring av bestämmelserna.

Vilken typ av uppgifter som hänförs till kategorin känsliga personuppgifter har emellertid utökats genom dataskyddsförordningen. Numera ingår även sexuell läggning och genetiska uppgifter i begreppet. Även biometriska uppgifter för att entydigt identifiera en fysisk person har tillkommit.

Vi anser att det är en självklarhet att sexuell läggning bör omfattas av utlänningsdatalagens bestämmelse om behandling av känsliga personuppgifter.

Genetiska uppgifter definieras, enligt artikel 4.13 i dataskyddsförordningen, i korthet som ”alla personuppgifter som rör nedärvda eller förvärvade genetiska kännetecken för en fysisk person”. Biometriska uppgifter är, enligt artikel 4.14, sådana personuppgifter som har 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. Som uttryckliga exempel på biometriska uppgifter nämns i dataskyddsförordningen ansiktsbilder och fingeravtrycksuppgifter. Det är enligt vår mening svårt att förutse hur den tekniska utvecklingen kommer att förändra möjligheten att behandla personuppgifter i verksamhetssystemen. Vi gör därför bedömningen att även genetiska uppgifter och biometriska uppgifter för att entydigt identifiera en fysisk person bör ingå i utlänningsdatalagens uppräkningslista av de känsliga personuppgifter där behandlingen är begränsad.

Ovanstående åstadkoms enligt vår uppfattning lättast genom att låta utlänningsdatalagens definition av känsliga personuppgifter innehålla en hänvisning till artikel 9.1 i dataskyddsförordningen, där de kategorier av personuppgifter som anses vara känsliga räknas upp. En sådan lagstiftningsteknik används även i Dataskyddsutredningens förslag till dataskyddslag. På detta sätt undviks användningen av ordet *ras* i utlänningsdatalagen, vilket är i överens-



stämmelse med det förslag som nyligen lämnats i betänkandet av Utredningen om transpersoners straffrättsliga skydd m.m. (SOU 2015:103 s. 165 ff.).

Den hänvisning till dataskyddsförordningens definition av känsliga personuppgifter som vi föreslår får till följd att användningsbegränsningen i 15 § kommer att gälla även för exempelvis fotografier som entydigt kan identifiera en person. Sådana fotografier kommer därmed inte längre att kunna användas i exempelvis testverksamhet, om de inte finns i det speciella registret över fingeravtryck och fotografier (se nedan). Vi anser att detta är rimligt, eftersom denna typ av personuppgifter enligt dataskyddsförordningen ingår bland de personuppgifter som anses vara särskilt integritetskänsliga. Vi vill emellertid påpeka att det inte är alla fotografier som förekommer i ett ärende som kommer att omfattas av ändamålsbegränsningen. Bestämmelsen kommer endast att gälla för de fotografier som är sådana att man med hjälp av dem *entydigt* kan identifiera en fysisk person. Ett pass som av Migrationsverket bedöms vara undermåligt ur bevissynpunkt kan enligt vår mening exempelvis inte entydigt identifiera en person. Detsamma gäller rimligen för t.ex. bröllopfoton och andra familjerelaterade fotografier.

Det faktum att fingeravtryck och fotografier enligt dataskyddsförordningens definition numera ingår i kategorin känsliga personuppgifter innebär vidare att det krävs redaktionella ändringar i utlänningsdatalagen. Vi föreslår att lagens bestämmelse om vilka förutsättningar som gäller för behandling av känsliga personuppgifter (15 §) kompletteras med en upplysning om att känsliga personuppgifter även får behandlas med stöd av den bestämmelse som reglerar Migrationsverkets rätt att föra register över fingeravtryck och fotografier (nuvarande 14 §). Detta innebär att uppgifter i form av fingeravtryck och fotografier som förekommer i det speciella registret alltså får användas för exempelvis testverksamhet. För att utlänningsdatalagens bestämmelser om känsliga personuppgifter ska ha en logisk inbördes ordning föreslår vi också att 14 § med tillhörande rubrik flyttas till en ny paragraf närmast efter 15 §.

## 12.2 Sökbegränsningar

### 12.2.1 Utlänningsdatalagen och dataskyddslagen

En vanligt förekommande skyddsåtgärd i registerförfattningar är sökbegränsningar. Dataskyddsutredningen har föreslagit att det som en huvudregel för svenska myndigheter ska finnas sökbegränsningar för känsliga personuppgifter. Bestämmelsen finns i den föreslagna 3 kap. 4 § dataskyddslagen.<sup>4</sup>

Av 17 § utlänningsdatalagen framgår att det vid sökning i personuppgifter är förbjudet att som sökbegrepp använda uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa eller sexualliv. Dessa kategorier av personuppgifter motsvarar i sin helhet de som enligt 13 § PuL betecknas som känsliga. Bestämmelserna i 17 § utlänningsdatalagen har enligt förarbetena (prop. 2015/16:65 s. 85) införts för att minimera riskerna för att känsliga personuppgifter missbrukas och för att upprätthålla integritetsskyddet.

Utlänningsdatalagen innehåller sökbegränsningar även för personuppgifter som till sin art inte betecknas som känsliga. Enligt 18 § första stycket utlänningsdatalagen är det vid behandling av personuppgifter för ändamål som anges i 12 § 2 den lagen (information som rör förhållanden i andra länder) förbjudet att som sökbegrepp använda personuppgifter som direkt pekar ut den registrerade. Av bestämmelsens andra stycke framgår vidare att sådana uppgifter om lagöverträdelser m.m. som anges i 21 § PuL inte får användas som sökbegrepp. Undantag görs dock för uppgifter om beslut om förvar enligt utlänningslagen (2005:716). Bestämmelsen i 21 § PuL avser personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden, vilka enligt bestämmelsens huvudregel endast får behandlas av myndigheter.

När dataskyddsförordningen börjar tillämpas kommer personuppgiftslagen att upphävas.<sup>5</sup> Dataskyddsutredningen har emellertid föreslagit att det i dataskyddslagen ska införas en bestämmelse

<sup>4</sup> Se Dataskyddsutredningens betänkande (SOU 2017:39 s. 179).

<sup>5</sup> Se kommittédirektiv till Dataskyddsutredningen (Dir 2016:15 s. 6).

(3 kap. 9 §) som innebär att personuppgifter som rör fällande domar i brottmål, lagöverträdelser som innefattar brott eller straffprocessuella tvångsmedel endast får behandlas av myndigheter. Bestämmelsen utgör ett införlivande av artikel 10 i dataskyddsförordningen.

### 12.2.2 Bedömning

**Förslag:** Det ska vara förbjudet att vid sökning i personuppgifter använda sökbegrepp som avslöjar sådana särskilda kategorier av uppgifter som anges i artikel 9.1 i dataskyddsförordningen (känsliga personuppgifter).

Personuppgifter i Migrationsverkets register över fingeravtryck och fotografier ska dock även fortsättningsvis få behandlas enligt de nuvarande förutsättningarna.

**Bedömning:** I övrigt föranleder dataskyddsförordningen ingen ändring i sak av utlänningsdatalagens bestämmelser om sök begränsningar. Begränsningar för uppgifter om lagöverträdelser m.m. bör finnas kvar.

Vid utlänningsdatalagens tillkomst identifierades ett antal sökbegrepp som bedömdes medföra särskilda integritetsrisker på lagens tillämpningsområde. Utöver känsliga personuppgifter handlar det om uppgifter som direkt pekar ut en person vid sökning i landinformation samt uppgifter om lagöverträdelser m.m. såsom de framgår av 21 § PuL.

Sök begränsningar utgör en skyddsåtgärd i dataskyddsförordningens mening. Det finns inte någon bestämmelse i förordningen som föranleder ändring vad gäller förekomsten av sök begränsningar i utlänningsdatalagen. Inom utlänningsdatalagens tillämpningsområde behandlas vidare stora mängder känsliga personuppgifter och det finns en möjlighet för allmänheten att med stöd av tryckfrihetsförordningen begära ut sammanställningar av integritetskänsliga personuppgifter, om en sådan sammanställning är tillåten att göra för en myndighet. Utifrån dessa aspekter är det enligt vår mening önskvärt att behålla det skydd för känsliga personuppgifter som sök begränsningarna utgör. Samma

resonemang gäller naturligtvis för de övriga integritetskänsliga uppgifter som träffas av de nuvarande sökbegränsningarna. Sökbegränsningar för känsliga personuppgifter skulle vidare följa den huvudregel som Dataskyddsutredningen genom 3 kap. 4 § dataskyddslagen har föreslagit för svenska myndigheter.<sup>6</sup>

Bestämmelsen i 17 § utlänningsdatalagen, som anger att det är förbjudet att använda känsliga personuppgifter som sökbegrepp, bör dock ändras med hänsyn till att det i dataskyddsförordningen har tillkommit kategorier av personuppgifter som ska anses vara känsliga. I detta fall görs ändringen enligt vår mening enklast genom en hänvisning till den paragraf i utlänningsdatalagen där det kommer att finnas en hänvisning till dataskyddsförordningens definition av begreppet känsliga personuppgifter (se avsnitt 12.1.5). Därutöver föreslår vi en mindre redaktionell ändring av 17 § utlänningsdatalagen, som dock inte är avsedd att utgöra någon ändring i sak. För att även fortsättningsvis möjliggöra de nu tillåtna sökningarna i Migrationsverkets register över fingeravtryck och fotografier bör det i bestämmelsen vidare anges att sökförbudet inte hindrar att personuppgifter behandlas med stöd av den bestämmelse som reglerar Migrationsverkets rätt att föra register över fingeravtryck och fotografier (nuvarande 14 §).

Det är också nödvändigt att ändra 18 § andra stycket utlänningsdatalagen, som förbjuder användning av lagöverträdelse m.m. som sökbegrepp. De begrepp som avses definieras för närvarande – genom en hänvisning till 21 § PuL – som lagöverträdelse som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel och administrativa frihetsberövanden. Den motsvarande bestämmelse som föreslagits i dataskyddslagen (3 kap. 9 §) motsvarar inte fullt ut personuppgiftslagens definition, eftersom den endast omfattar de domar som är fällande och inte heller omfattar administrativa frihetsberövanden.

Bestämmelserna i 21 § PuL och 3 kap. 9 § dataskyddslagen reglerar emellertid vilka kategorier av uppgifter som endast får behandlas av myndigheter. Detta innebär att utlänningsdatalagens bestämmelse om sökbegränsningar inte måste motsvara den nya bestämmelsen i dataskyddslagen. Något annat har inte heller framkommit än att de tidigare övervägandena kring vilka

---

<sup>6</sup> Se Dataskyddsutredningens betänkande (SOU 2017:39).

sök begränsningar som bör finnas inom utlänningsdatalagens tillämpningsområde fortfarande är relevanta. Mot den bakgrunden föreslår vi att utlänningsdatalagens bestämmelse om sök begränsningar gällande lagöverträdelser m.m. bör finnas kvar oförändrad. Detta medför emellertid redaktionella ändringar, eftersom de förbjudna sökbegreppen (lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel och administrativa frihetsberövanden) måste framgå direkt av utlänningsdatalagens bestämmelse.



## 13 Tillgången till personuppgifter

### 13.1 Utlänningsdatalagen och utlänningsdataförordningen

Enligt 16 § första stycket utlänningsdatalagen ska tillgången till personuppgifter begränsas till det som varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Av andra stycket i samma bestämmelse framgår att regeringen eller den myndighet som regeringen bestämmer med stöd av 8 kap. 7 § regeringsformen kan meddela närmare föreskrifter om tillgången till personuppgifter.

Av 4 § utlänningsdataförordningen framgår att det vid tilldelning av behörighet för tillgång till personuppgifter särskilt ska beaktas att det, utöver behovet av uppgifterna, ställs krav på utbildning och erfarenhet. Migrationsverket, Polismyndigheten och utlandsmyndigheterna ansvarar vidare, enligt 7 § utlänningsdataförordningen, för att det inom den egna myndigheten finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheter för tillgång till personuppgifter. Migrationsverket ansvarar också för att det finns sådana rutiner hos utlandsmyndigheterna för den behandling av personuppgifter som sker under Migrationsverkets personuppgiftsansvar.<sup>1</sup>

Utlänningsdataförordningen innehåller även en vidaredelegering av föreskrifträtten vad gäller tillgången till personuppgifter. Enligt 5 § första stycket och 6 § får Migrationsverket och Polismyndigheten meddela närmare föreskrifter om tillgången till personuppgifter för personer som är verksamma inom respektive myndighet. Av 5 § andra stycket framgår också att Migrationsverket, efter att ha gett Regeringskansliet (Utrikesdepartementet)

---

<sup>1</sup> Migrationsverket är personuppgiftsansvarigt för den automatiserade personuppgiftsbehandling som utförs av utlandsmyndigheterna, se nuvarande 9 § utlänningsdatalagen och kapitel 10.

tillfälle att yttra sig, får meddela närmare föreskrifter om tillgången till personuppgifter som behandlas av utlandsmyndigheterna under Migrationsverkets personuppgiftsansvar.

Såvitt vi känner till har varken Migrationsverket eller Polismyndigheten utnyttjat föreskriftsrätten enligt utlänningsdataförordningen.

## 13.2 Bedömning

**Bedömning:** Dataskyddsförordningen föranleder ingen ändring av utlänningsdatalagens och utlänningsdataförordningens bestämmelser om tillgången till personuppgifter.

Den personuppgiftsansvarige har, enligt artikel 24.1 och artikel 32 i dataskyddsförordningen, skyldighet att se till att en lämplig säkerhetsnivå för behandlingen av personuppgifter upprätthålls. Detta ska, enligt samma bestämmelser, ske bl.a. genom att den personuppgiftsansvarige vidtar lämpliga tekniska och organisatoriska åtgärder. Den personuppgiftsansvariges skyldigheter i denna del återfinns även i de allmänna principer för behandling av personuppgifter som framgår av artikel 5.1 f i dataskyddsförordningen.

Vi har gjort bedömningen att sökbegränsningar utgör en säkerhetsåtgärd i dataskyddsförordningens mening (se avsnitt 12.2.2). Detsamma gäller enligt vår mening bestämmelser om behörighetsbegränsningar, tilldelningsstyrning och andra rutiner som säkerställer att personuppgiftsbehandlingen sker i enlighet med dataskyddsförordningen.

Åtgärder som säkerställer en lämplig säkerhetsnivå ska förvisso vidtas av de personuppgiftsansvariga även utan bestämmelser i registerförfattningar. Bestämmelser om vilka säkerhetsåtgärder som ska vidtas i en viss verksamhet utgör dock enligt vår mening sådana specifika krav på personuppgiftsbehandling som enligt artikel 6.2 i dataskyddsförordningen får fastställas genom nationella registerförfattningar (se kapitel 5).

Att det finns säkerhetsåtgärder för personuppgiftsbehandlingen är vidare en förutsättning för att känsliga personuppgifter ska få behandlas för ett viktigt allmänt intresse med stöd av undantaget i



artikel 9.2 g i dataskyddsförordningen. Av avsnitt 12.1.5 framgår att detta undantag har stor betydelse för de myndigheter som behandlar personuppgifter inom utlänningsdatalagens tillämpningsområde. Det faktum att en säkerhetsåtgärd kommer till uttryck i en registerförfattning säkerställer enligt vår mening skyddsåtgärden på ett sådant sätt som avses i artikel 9.2 g i dataskyddsförordningen.

I avsnitt 18.2 gör vi bedömningen att dataskyddsförordningen inte hindrar att nationella bestämmelser om personuppgiftsbehandling införs i en förordning eller i en myndighetsföreskrift, så länge föreskrifterna har tillkommit i laga ordning.

Mot den bakgrunden bedömer vi att bestämmelserna om tillgången till personuppgifter i 16 § utlänningsdatalagen och 4–7 §§ utlänningsdataförordningen är förenliga med dataskyddsförordningen och bör kvarstå i sin nuvarande lydelse.

Vi vill i detta sammanhang betona att förekomsten av behörighetsbegränsningar m.m. i en registerförfattning inte innebär att man kan bortse från de övriga krav på lämpliga säkerhetsåtgärder som dataskyddsförordningen föreskriver. Som ett exempel kan nämnas att förordningen ställer krav på att dataskydd byggs in i databehandlingssystem i den utsträckning det är lämpligt med hänsyn till bl.a. kostnader, behandlingens art och omfattning och de risker som behandlingen innebär (artikel 25). Som ett exempel på ett sådant inbyggt dataskydd kan nämnas loggning.



# 14 Den registrerades rättigheter

## 14.1 Inledande kommentar

Utlänningsdatalagen innehåller inga egna bestämmelser om de registrerades rättigheter. I stället hänvisas i 8 § första stycket 5, 6 och 12 utlänningsdatalagen till 23, 25–28 och 48 §§ PuL. Dessa bestämmelser reglerar den registrerades rätt till information, rättelse, blockering och utplåning av personuppgifter samt den registrerades rätt till skadestånd. När dataskyddsförordningen börjar tillämpas kommer personuppgiftslagen att upphävas.<sup>1</sup> Samtliga hänvisningar till personuppgiftslagen måste därmed utgå.

Dataskyddsförordningens bestämmelser om de registrerades rättigheter finns i artiklarna 12–22 och 34. Artikel 12 innehåller övergripande bestämmelser om bl.a. hur och i vilken form information ska lämnas till de registrerade samt tidsfristerna för detta. I artiklarna 13–22 och 34 regleras därefter de registrerades rättigheter relativt detaljerat.

Inledningsvis kan vi konstatera att artikel 20, som gäller rätten till dataportabilitet, inte är tillämplig på personuppgiftsbehandling inom utlänningsdatalagens tillämpningsområde, eftersom behandling av personuppgifter enligt lagen inte grundar sig på samtycke eller avtal (se artikel 20.1 a).

Vad gäller de registrerades resterande rättigheter enligt dataskyddsförordningen är vår avsikt inte att i detta kapitel göra en heltäckande genomgång. Vårt syfte är i stället att lyfta fram de viktigaste förändringarna för de myndigheter som omfattas av utlänningsdatalagen. Det är enligt vår mening vidare av största vikt att de aktuella myndigheternas ärendehandläggning inte avstannar och att de personuppgifter som hanteras inom ramen för

---

<sup>1</sup> Se kommittédirektiv till Dataskyddsutredningen (Dir 2016:15 s. 6).

myndigheternas ärenden kan arkiveras när ärendet är avgjort. Mot den bakgrunden har vi även för avsikt att i detta kapitel analysera dataskyddsförordningens möjligheter att begränsa de registrerades rättigheter och bedöma behovet av att införa sådana begränsningar.

## 14.2 En generell möjlighet till undantag

De rättigheter som regleras i artiklarna 13–22 och 34 i dataskyddsförordningen innehåller i vissa fall undantag som endast gäller för den enskilda rättigheten. Dessa redogör vi för i kommande avsnitt. I artikel 23 i dataskyddsförordningen finns emellertid även en generell bestämmelse som ger medlemsstaterna vissa möjligheter att i den nationella lagstiftningen införa undantag från rättigheterna i artiklarna 12–22 samt 34 i förordningen. En sådan begränsning måste ske med respekt för andemeningen i de grundläggande rättigheterna och friheterna. Den måste också utgöra en nödvändig och proportionell åtgärd i ett demokratiskt samhälle. Begränsningen får vidare endast ske i syfte att säkerställa vissa intressen, som räknas upp i artikel 23.1 a–j. För den verksamhet som utförs inom ramen för utlänningsdatalagens tillämpningsområde är det enligt vår mening led e som främst kommer i fråga. Enligt detta led får en begränsning av de registrerades rättigheter ske i syfte att säkerställa ”en medlemsstats viktiga mål av generellt allmänt intresse”. Som exempel på sådana mål nämns viktiga ekonomiska eller finansiella intressen, där penning-, budget- eller skattefrågor ingår, men även folkhälsa och social trygghet.

De undantag som införs i nationell rätt med stöd av artikel 23.1 i dataskyddsförordningen ska vidare, enligt punkt två i samma artikel, när det är relevant innehålla specifika bestämmelser om bl.a. ändamålen med behandlingen, omfattningen av de införda begränsningarna, skyddsåtgärder för att förhindra missbruk, specificering av den personuppgiftsansvarige, lagringstid och tillämpliga skyddsåtgärder. Detta är bestämmelser som enligt vår bedömning ofta återfinns i svenska registerförfattningar. Som exempel nämns också bestämmelser om de registrerades rätt att bli informerade om begränsningen, såvida detta inte inverkar menligt på begränsningen.

## 14.3 Information när personuppgifter samlas in från den registrerade

### 14.3.1 Utlänningsdatalagen och personuppgiftslagen

Utlänningsdatalagen hänvisar, genom 8 § första stycket 5, till 23, 25 och 27 §§ PuL. Enligt 23 § PuL ska den personuppgiftsansvarige självmant lämna den registrerade information om behandlingen av personuppgifter när dessa samlas in från den registrerade själv. Informationen ska lämnas i samband med att uppgifterna samlas in. Vad gäller uttrycket *insamling av personuppgifter* kan sägas att detta inte bara torde avse situationer där uppgifter lämnas till en myndighet på begäran av myndigheten, utan även t.ex. när myndigheten får personuppgifter genom att den enskilde självmant lämnar in dem.<sup>2</sup>

I 25 § PuL regleras mer detaljerat vilken information som ska lämnas till den registrerade i en sådan situation. Informationen ska omfatta uppgift om den personuppgiftsansvariges identitet, om ändamålen med behandlingen och all övrig information som behövs för att den registrerade ska kunna ta till vara sina rättigheter i samband med behandlingen. Som exempel på sådan övrig information nämns mottagarna av uppgifterna, skyldigheten att lämna uppgifter och rätten att ansöka om information och få rättelse. Information behöver dock inte lämnas om sådant som den registrerade redan känner till.

Den personuppgiftsansvariges informationsplikt begränsas dock av 27 § PuL. Här stadgas att bestämmelserna i 23 och 25 §§ PuL inte gäller om 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.

### 14.3.2 Dataskyddsförordningen och dataskyddslagen

Enligt artikel 13 i dataskyddsförordningen har en registrerad rätt att få relativt utförlig information från den personuppgiftsansvarige när personuppgifterna samlats in från den registrerade själv. Informationen ska bl.a. innefatta den personuppgiftsansvariges

---

<sup>2</sup> Jfr förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 39).

identitet och kontaktuppgifter, kontaktuppgifter till dataskyddsombudet, uppgift om den period under vilken personuppgifterna kommer att lagras eller de kriterier som används för att fastställa denna period, information om rätten att ge in klagomål till tillsynsmyndigheten och om rätten att begära rättelse, radering eller begränsning av behandling av personuppgifterna. Informationen ska lämnas när den personuppgiftsansvarige får personuppgifterna. Den personuppgiftsansvarige behöver dock inte lämna sådan information som den registrerade redan förfogar över.

Enligt Dataskyddsutredningens bestänkande (SOU 2017:39) ska dataskyddslagen i 5 kap. 1 § innehålla en bestämmelse enligt vilken den registrerades rätt till information och tillgång till personuppgifter enligt artiklarna 13–15 i dataskyddsförordningen inte gäller sådana uppgifter som den personuppgiftsansvarige, enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning, inte får lämna ut till den registrerade. Förslaget innebär att det undantag för vissa sekretessbelagda uppgifter som nu finns i 27 § PuL kommer att finnas kvar även när dataskyddsförordningen börjar tillämpas.

### 14.3.3 Bedömning

**Förslag:** Den registrerades rätt till information enligt artikel 13 i dataskyddsförordningen ska inte gälla 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. Regleringen ska genomföras genom en hänvisning till den föreslagna 5 kap. 1 § första stycket dataskyddslagen.

Artikel 13 i dataskyddsförordningen reglerar vilka uppgifter den personuppgiftsansvarige ska lämna till en registrerad när uppgifter samlats in från den registrerade själv. Exempel på situationer där de aktuella myndigheterna samlar in personuppgifter från den enskilde själv är när de tar emot ansökningar, skrivelser och svar på förfrågningar. Även om uppgifterna kommer från en ställföreträdare eller ett ombud som har i uppdrag att företräda den registrerade

bör uppgifterna i dessa situationer bedömas ha samlats in från den registrerade själv.<sup>3</sup>

Artikel 13 i dataskyddsförordningen liknar till sin uppbyggnad 23 och 25 §§ PuL. En avgörande skillnad mellan dataskyddsförordningens och personuppgiftslagens reglering är att förordningen är mycket mer utförlig när det gäller vilken information som ska lämnas till den registrerade. Precis som enligt personuppgiftslagen görs dock undantag från den personuppgiftsansvariges informationsskyldighet om den registrerade redan förfogar över den information som ska lämnas.

Vi anser att den registrerade möjligtvis kan anses ha kännedom om vem som är personuppgiftsansvarig och om de ändamål som uppgifterna ska behandlas för. Vem som är personuppgiftsansvarig framgår av utlänningsdatalagen och ändamålet framgår ofta av sammanhanget – om uppgifterna samlas in i ett enskilt ärende är det underförstått att uppgifterna används för handläggningen av detsamma. Däremot anser vi inte att den registrerade kan antas känna till exempelvis vem som är myndighetens dataskyddsombud eller kriterierna för att fastställa under vilken period uppgifterna kommer att lagras. Även om den registrerades rätt att begära rättelse och radering m.m. framgår av dataskyddsförordningen kan den registrerade enligt vår mening inte heller anses föfoga över denna information. Om tanken vore att bestämmelserna skulle tolkas på detta vis hade någon skyldighet för den personuppgiftsansvarige att lämna information om dessa rättigheter rimligen inte förts in i dataskyddsförordningen.

När de aktuella myndigheterna samlar in personuppgifter från den registrerade själv kan han eller hon enligt vår uppfattning således inte anses föfoga över all den information som ska lämnas enligt artikel 13 i dataskyddsförordningen. Beroende på vilken information som lämnas till de registrerade i nuläget skulle det därmed kunna finnas anledning för myndigheterna att se över sina rutiner i denna del. Detta är emellertid ett arbete som sker på verkställighetsnivå och som inte ligger inom ramen för vårt uppdrag att behandla.

---

<sup>3</sup> Sören Öman och Hans-Olof Lindblom, Personuppgiftslagen (15 september 2016, Zetco), kommentar till 23 §.

Dataskyddsförordningens bestämmelser skulle enligt vår bedömning sammanfattningsvis kunna innebära att myndigheterna behöver utöka den information som ges till de registrerade när personuppgifter samlas in från dem. Endast en ökad administrativ belastning innebär enligt vår mening emellertid inte att det finns möjlighet att begränsa de registrerades rättigheter med stöd av artikel 23 i dataskyddsförordningen. Anledningen är att begränsningen i sådant fall inte skulle göras i syfte att säkerställa viktiga mål av generellt allmänt intresse eller något annat av de syften som räknas upp i artikel 23.1 a–j. Någon annan möjlighet till en generell begränsning finns inte.

En hänvisning bör enligt vår mening dock göras i utlänningsdatalagen till den föreslagna 5 kap. 1 § dataskyddslagen, som innebär att den rätt till information som den registrerade har enligt bl.a. artikel 13 i dataskyddsförordningen inte gäller uppgifter som enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning inte får lämnas ut till den registrerade. På detta sätt upprätthålls det förhållande som nu gäller, nämligen att bestämmelser om sekretess eller tystnadsplikt går före den registrerades rätt att få information om behandlingen av hans eller hennes personuppgifter.

## **14.4 Information när personuppgifter samlas in från någon annan än den registrerade**

### **14.4.1 Utlänningsdatalagen och personuppgiftslagen**

Enligt 24 § första stycket PuL ska den personuppgiftsansvarige självant lämna den registrerade information om behandlingen av personuppgifter när uppgifterna samlats in från någon annan källa än den registrerade själv. Enligt 24 § andra stycket behöver information till den registrerade emellertid inte lämnas om det finns bestämmelser om registrerandet eller utlämnandet av personuppgifterna i lag eller annan författning.

I förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 50) gjorde regeringen bedömningen att någon hänvisning till 24 § PuL inte behöver tas in i utlänningsdatalagen. Som skäl för detta framfördes att det kommer att finnas bestämmelser om registrerandet eller utlämnandet av personuppgifterna i utlänningsdatalagen.



### 14.4.2 Dataskyddsförordningen

Enligt artikel 14 i dataskyddsförordningen ska relativt utförlig information lämnas till den registrerade när den personuppgiftsansvarige har fått personuppgifterna från någon annan källa än den registrerade själv. Artikel 14.5 c innehåller dock – liksom 24 § PuL – undantag som innebär att den personuppgiftsansvarige inte behöver lämna sådan information, om den personuppgiftsansvarige har rätt att ta emot eller lämna ut uppgifterna enligt medlemsstatens nationella rätt. En förutsättning för att undantaget ska vara tillämpligt är att den nationella rätten fastställer lämpliga åtgärder för att skydda den registrerades berättigade intressen. Någon ledning gällande vilken typ av skyddsåtgärder det kan röra sig om finns inte i skälen till förordningen.

### 14.4.3 Bedömning

**Bedömning:** Personuppgiftsbehandlingen inom utlänningsdatalagens tillämpningsområde omfattas av undantaget i artikel 14.5 c i dataskyddsförordningen från skyldigheten att lämna information när personuppgifter har getts in från någon annan än den registrerade själv.

Artikel 14 i dataskyddsförordningen reglerar vilken information som ska lämnas till den registrerade när personuppgifter samlats in från annan än den registrerade själv. Detta bör, enligt vår bedömning, förekomma främst i de aktuella myndigheternas ärendehandläggning, exempelvis när den sökande i ett ärende om uppehållstillstånd lämnar in uppgifter om sina släktförhållanden eller när resultatet av en DNA-analys eller en åldersbedömning kommer in till Migrationsverket från den externa aktör som utfört utredningsåtgärden. Migrationsverket, Polismyndigheten och utlandsmyndigheterna får enligt utlänningsdatalagen behandla de personuppgifter som behövs för de primära ändamålen, t.ex. för handläggning av de ärenden som träffas av lagens tillämpningsområde. Mot den bakgrunden anser vi att den personuppgiftsbehandling som sker inom utlänningsdatalagens tillämpningsområde omfattas av undantaget i artikel 14.5 c i dataskydds-

förordningen. Detta innebär i sin tur att myndigheterna inte är skyldiga att lämna information till de registrerade i dessa situationer.

Utlänningsdatalagen innehåller vidare en mängd bestämmelser som skyddar den registrerades integritet när myndigheterna behandlar personuppgifter. Som exempel kan nämnas bestämmelser om sök- och behörighetsbegränsningar samt direktåtkomst. Enligt vår bedömning finns det därmed i nationell rätt ett tillräckligt skydd för den registrerades intressen för att undantaget i artikel 14.5 c i dataskyddsförordningen ska kunna tillämpas inom utlänningsdatalagens tillämpningsområde. Det behövs enligt vår mening därmed inte någon ytterligare lagstiftningsåtgärd för att myndigheterna ska kunna tillämpa undantaget.

## 14.5 Information efter begäran

### 14.5.1 Utlänningsdatalagen och personuppgiftslagen

Utlänningsdatalagen hänvisar, genom 8 § första stycket 5, till 26 och 27 §§ PuL. Enligt 26 § första stycket PuL är den personuppgiftsansvarige skyldig att, efter begäran, en gång per kalenderår lämna besked om huruvida personuppgifter som rör den sökande behandlas eller inte (ett s.k. registerutdrag). Om sådana uppgifter behandlas ska den registrerade också få information om vilka uppgifter som behandlas, varifrån de har hämtats, ändamålen med behandlingen och till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut.

Enligt 26 § tredje stycket PuL behöver sådan information inte lämnas vad gäller 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. Inte heller gäller undantaget för löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats under längre tid än ett år.

Den personuppgiftsansvariges informationsplikt begränsas av 27 § PuL. Enligt denna bestämmelse gäller inte skyldigheten i 26 § PuL om 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.

### 14.5.2 Dataskyddsförordningen och dataskyddslagen

Enligt artikel 15 i dataskyddsförordningen har den registrerade rätt att av den personuppgiftsansvarige få bekräftelse på om personuppgifter som rör honom eller henne håller på att behandlas. Om så är fallet har den registrerade rätt till relativt utförlig information om behandlingen av dessa personuppgifter. Information ska bl.a. lämnas om ändamålen med behandlingen, vilka kategorier av uppgifter som behandlas, mottagarna av uppgifterna, den period under vilken uppgifterna kommer att lagras eller kriterierna för att fastställa denna period, rätten att begära rättelse eller radering av uppgifterna samt rätten att ge in klagomål till en tillsynsmyndighet. Några undantag från rätten att få information om personuppgiftsbehandlingen efter begäran finns inte i artikel 15.

Av artikel 12.5 framgår att utgångspunkten är att information enligt bl.a. artikel 15 ska tillhandahållas kostnadsfritt. Det framgår dock även att om en begäran är uppenbart ogrundad eller orimlig, särskilt på grund av dess repetitiva art, får den personuppgiftsansvarige antingen ta ut en rimlig avgift eller vägra att tillmötesgå begäran. Det är den personuppgiftsansvarige som ska visa att en begäran är uppenbart ogrundad eller orimlig. Av skäl 63 till förordningen framgår att de registrerade bör ha rätt att få tillgång till personuppgifter på detta sätt med rimliga intervall.

Enligt Dataskyddsutredningens förslag (SOU 2017:39) ska dataskyddslagen i 5 kap. 2 § innehålla en bestämmelse som motsvarar undantaget i 26 § tredje stycket PuL för personuppgifter i löpande text som inte fått sin slutliga utformning eller som utgör minnesanteckningar. Vidare ska dataskyddslagen, enligt Dataskyddsutredningens förslag, i 5 kap. 1 § innehålla en bestämmelse enligt vilken bl.a. artikel 15 i dataskyddsförordningen inte gäller uppgifter som, enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning, inte får lämnas ut till den registrerade.

### 14.5.3 Bedömning

**Förslag:** Den registrerades rätt till information enligt artikel 15 i dataskyddsförordningen ska inte gälla 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. Regleringen ska genomföras genom en hänvisning till den föreslagna 5 kap. 1 § första stycket dataskyddslagen.

Den registrerades rätt till tillgång till personuppgifter enligt artikel 15 i dataskyddsförordningen ska inte gälla personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande. Undantaget ska inte gälla om personuppgifterna har lämnats ut till tredje part, behandlas enbart för arkivändamål av allmänt intresse eller statistiska ändamål eller har behandlats under längre tid än ett år i löpande text som inte fått sin slutliga utformning. Regleringen ska genomföras genom en hänvisning till den föreslagna 5 kap. 2 § dataskyddslagen.

Den information som ska lämnas till den registrerade enligt artikel 15 i dataskyddsförordningen är något mer utförlig än den som i nuläget ska lämnas i enlighet med utlänningsdatalagen och personuppgiftslagen. För de informationspunkter som är nya (t.ex. perioden för lagring samt information om möjligheten att begära rättelse och radering) bör det enligt vår mening vara möjligt att ta fram standardiserad information som kan användas vid de flesta förfrågningar. Detta borde innebära att de nya bestämmelserna inte medför en alltför stor administrativ belastning för de aktuella myndigheterna.

Som vi nämnt i avsnitt 14.5.2 innehåller artikel 15 i dataskyddsförordningen inte några undantag från rätten att få information om personuppgiftsbehandlingen efter begäran. Vi anser dock att en hänvisning bör göras i utlänningsdatalagen till den föreslagna 5 kap. 1 § första stycket dataskyddslagen. Den bestämmelsen innebär att artiklarna 13–15 i dataskyddsförordningen inte gäller uppgifter som, enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning, inte får lämnas ut till den

registrerade.<sup>4</sup> På detta sätt kommer bestämmelser om sekretess eller tystnadsplikt att gå före den registrerades rätt att få information om behandlingen av hans eller hennes personuppgifter även när dataskyddsförordningen börjar tillämpas.

Vi anser vidare att det bör göras en hänvisning i utlänningsdatalagen till den föreslagna 5 kap. 2 § dataskyddslagen, som motsvarar 26 § tredje stycket PuL. Genom en sådan hänvisning kommer de aktuella myndigheternas tjänstemän även framöver att under en rimlig tid få ha sina ofärdiga alster i fred. På samma sätt som i nuläget måste detta enligt vår mening anses vara en rimlig avvägning mellan den registrerades rätt till information och myndigheternas verksamhetsbehov.

Slutligen anser vi att det inte finns anledning att i utlänningsdatalagen införa bestämmelser som begränsar den registrerades rättigheter enligt artikel 15 i dataskyddsförordningen ytterligare. Genom de hänvisningar till 5 kap. 1 och 2 §§ dataskyddslagen som vi föreslagit kommer samma undantag som i dag att gälla. Vi kan inte se att det finns några ytterligare behov av att begränsa rättigheterna för att säkerställa viktiga mål av generellt allmänt intresse eller något annat av de syften som framgår av artikel 23.1 dataskyddsförordningen.

## **14.6 Rättelse och radering samt rätt att göra invändningar och begära begränsning av behandling**

### **14.6.1 Utlänningsdatalagen, personuppgiftslagen och 1995 års dataskyddsdirektiv**

Utlänningsdatalagen hänvisar, genom 8 § 6, till 28 § PuL. Enligt denna bestämmelse 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 den lagen. Om den registrerade begär det ska den personuppgiftsansvarige också underrätta mottagarna av uppgifterna om

---

<sup>4</sup> Se Dataskyddsutredningens betänkande (SOU 2017:39).

åtgärden. Detsamma gäller om mera betydande skada eller olägenhet för den registrerade skulle kunna undvikas genom en sådan underrättelse. Underrättelse behöver dock inte lämnas om det visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

I utlänningsdatalagen nämns endast att hänvisningen till 28 § PuL gäller bestämmelsen om rättelse. Av förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 50) framgår dock att hänvisningen även avser rätten till blockering och utplåning av personuppgifter.

Utlänningsdatalagen hänvisar även, i 8 § 3, till bestämmelserna om grundläggande krav på behandling av personuppgifter i 9 § PuL. Enligt dessa bestämmelser ska den personuppgiftsansvarige se till att alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen.

Kort kan sägas att *rättelse* av en personuppgift innebär att en felaktig eller ofullständig uppgift ersätts av en uppgift om de rätta förhållandena eller att uppgifterna annars kompletteras. Med *blockering* avses en åtgärd som vidtas för att personuppgifterna ska förse med information om att de är spärrade och om anledningen till spärren, för att personuppgifterna inte ska lämnas ut till tredje man annat än med stöd av 2 kap. TF. *Utplånande* innebär helt enkelt att de aktuella personuppgifterna förstörs så att de inte kan återskapas.<sup>5</sup>

När personuppgifter behandlas för att utföra en arbetsuppgift av allmänt intresse eller som ett led i myndighetsutövning, ska medlemsstaterna enligt artikel 14 a i 1995 års dataskyddsdirektiv tillförsäkra den registrerade rätten att motsätta sig behandling av uppgifter som rör honom eller henne. Detta gäller emellertid endast om den nationella lagstiftningen inte föreskriver annat. Genom 12 § andra stycket PuL har lagstiftaren gjort den registrerades rätt att motsätta sig behandling mycket begränsad. Enligt denna bestämmelse har den registrerade endast rätt att motsätta sig sådan behandling av personuppgifter som är tillåten enligt personuppgiftslagen när behandlingen sker för ändamål som

---

<sup>5</sup> Sören Öman och Hans-Olof Lindblom, Personuppgiftslagen (15 september 2016, Zeteo), kommentaren till 28 §.

gäller direkt marknadsföring eller om behandlingen sker med stöd av samtycke.<sup>6</sup>

## 14.6.2 Dataskyddsförordningen

### Rättelse

Enligt artikel 16 i dataskyddsförordningen har den registrerade rätt att utan onödigt dröjsmål få felaktiga personuppgifter rättade. Den registrerade ska även, med beaktande av ändamålet med behandlingen, ha rätt att komplettera ofullständiga personuppgifter.

### Radering

Enligt artikel 17 i dataskyddsförordningen har den registrerade i vissa fall rätt att få sina personuppgifter raderade utan onödigt dröjsmål. Detta motsvarar personuppgiftslagens begrepp *utplåning*. De situationer som främst är av intresse inom utlänningsdatalagens tillämpningsområde är de som framgår av artikel 17.1 a, c och d i förordningen. Led a avser situationen att personuppgifterna inte längre är nödvändiga för de ändamål som de samlats in för eller på annat sätt behandlats för. Led c avser situationen att den registrerade har gjort invändningar mot behandlingen i enlighet med artikel 21.1 och det saknas berättigade skäl för behandlingen som väger tyngre än den registrerades skäl för radering. Led d avser situationen att personuppgifterna har behandlats på ett olagligt sätt.

Det finns dock en rad undantag från rätten till radering. De som enligt vår mening främst är av intresse är de som framgår av artikel 17.3 b och d i förordningen. Enligt led b har den registrerade inte rätt att få sina personuppgifter raderade om behandlingen av uppgifterna är nödvändig för att uppfylla en rättslig förpliktelse enligt unionsrätten eller en medlemsstats nationella rätt. Rätten till radering gäller inte heller om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den person-

---

<sup>6</sup> Se förarbetena till personuppgiftslagen (prop. 1997/98:44 s. 64 ff.).

uppgiftsansvariges myndighetsutövning. Den registrerade har vidare inte, enligt led d, rätt att få sina personuppgifter raderade om behandlingen är nödvändig för bl.a. arkivändamål av allmänt intresse eller statistiska ändamål, i den utsträckning som raderingen sannolikt omöjliggör eller avsevärt försvårar uppnåendet av syftet med den behandlingen.

### **Rätt att göra invändningar och begära begränsning av behandling**

Om behandlingen av personuppgifter grundar sig på en uppgift av allmänt intresse eller myndighetsutövning har den registrerade, enligt artikel 21.1 i dataskyddsförordningen, rätt att av skäl som hänför sig till hans eller hennes specifika situation göra invändningar mot behandlingen. Om en sådan invändning görs får den personuppgiftsansvarige inte längre behandla personuppgifterna om denne inte kan visa att det finns avgörande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter. Personuppgifterna får dock fortsätta behandlas bl.a. om det sker för fastställande, utövande eller försvar av rättsliga anspråk. Följden av att intresseavvägningen utfaller till den registrerades fördel blir, åtminstone om den registrerade begär det, att de aktuella personuppgifterna ska raderas. Detta framgår av artikel 17.1 c i dataskyddsförordningen.

Under den tid det tar för den personuppgiftsansvarige att efter en invändning kontrollera om den registrerades skäl mot behandlingen väger tyngre än den personuppgiftsansvariges skäl för att utföra behandlingen ska behandlingen av uppgifterna begränsas i enlighet med artikel 18.1 d.

Den registrerade har, enligt artikel 18.1 a–c i dataskyddsförordningen, även i vissa andra fall rätt att kräva att behandlingen av hans eller hennes personuppgifter begränsas. När den registrerade har gjort invändningar mot personuppgifternas riktighet ska behandlingen enligt led a begränsas under den tid då den personuppgiftsansvarige kontrollerar om personuppgifterna är riktiga. Enligt led b ska behandlingen begränsas om den är olaglig och den registrerade i stället för radering begär en begränsning av uppgifternas användning. Enligt led c ska behandlingen begränsas



om den personuppgiftsansvarige inte längre behöver personuppgifterna för ändamålen med behandlingen men de fortsatt behöver lagras eftersom den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

Under den tid begränsningen gäller får personuppgifterna, enligt huvudregeln i artikel 18.2, inte behandlas på annat sätt än att de lagras. Förfarandet motsvarar det som i personuppgiftslagen kallas *blockering*. Undantag finns dock, exempelvis får uppgifterna under begränsningsperioden behandlas för att fastställa rättsliga anspråk eller för skäl som rör ett viktigt allmänintresse för en medlemsstat.

### Mottagare ska underrättas

Enligt artikel 19 i dataskyddsförordningen ska den personuppgiftsansvarige underrätta varje mottagare av personuppgifterna om de rättelser, raderingar eller begränsningar av behandling som gjorts. Undantag från denna skyldighet får göras om det visar sig vara omöjligt eller medför en oproportionell ansträngning. Om den registrerade begär det ska den personuppgiftsansvarige även informera den registrerade om vilka mottagarna av personuppgifter är.

### 14.6.3 Bedömning

**Bedömning:** Det bör inte införas några undantag i utlänningsdatalagen från dataskyddsförordningens bestämmelser om de registrerades rättigheter i artiklarna 16–19 eller 21 och 22.

### Rättelse

Dataskyddsförordningens bestämmelser om de registrerades rätt att komplettera ofullständiga personuppgifter och få felaktiga personuppgifter rättade (artikel 16) motsvarar vad som, genom utlänningsdatalagens hänvisning till 9 och 28 §§ PuL, för närvarande gäller inom utlänningsdatalagens tillämpningsområde. Det bör enligt vår mening ligga i myndigheternas intresse att de

personuppgifter som behandlas i verksamheten är korrekta och fullständiga. Något behov av att på utlänningsdatalagens tillämpningsområde införa undantag från dataskyddsförordningens bestämmelse om rättelse finns enligt vår uppfattning därmed inte.

## Radering

Dataskyddsförordningens bestämmelser om rätten till radering är mer omfattande än vad som gäller enligt utlänningsdatalagen och personuppgiftslagen i dag. Enligt artikel 17.3 b i förordningen gäller rätten till radering dock inte om behandlingen är nödvändig som ett led i den personuppgiftsansvariges myndighetsutövning eller för att den personuppgiftsansvarige ska kunna utföra en uppgift av allmänt intresse. Som vi tidigare konstaterat (avsnitt 6.3.2) anser vi att den personuppgiftsbehandling som sker inom utlänningsdatalagens tillämpningsområde är nödvändig som ett led i myndighetsutövning eller i vart fall för att utföra en uppgift av allmänt intresse. Rätten till radering gäller enligt vår mening därför inte uppgifter i pågående ärenden. Undantaget i artikel 17.3 b garanterar därmed att handläggningen av öppna ärenden inte avstannar på grund av dataskyddsbestämmelser.

För arkivering finns dessutom, i artikel 17.3 d i dataskyddsförordningen, ett specifikt undantag från rätten till radering. Enligt denna bestämmelse ska den rätten inte gälla för det fall raderingen sannolikt omöjliggör eller avsevärt försvårar att syftet med den behandling som utförs för arkivändamål av allmänt intresse uppnås. Detta medför enligt vår mening att rätten till radering inte heller gäller personuppgifter som ingår i de handlingar som arkiverats i enlighet med gällande arkivlagstiftning. Vi anser att rätten till radering inte heller gäller för de personuppgifter som finns i avslutade ärenden som ännu inte har hunnit arkiveras. Bevarandet av allmänna handlingar är en förutsättning för allmänhetens möjlighet att ta del av dessa handlingar med stöd av tryckfrihetsförordningen, vilket enligt vår mening innebär att ett sådant bevarande är nödvändigt för en uppgift av allmänt intresse.

Eftersom redan befintliga undantag i dataskyddsförordningen enligt vår bedömning således garanterar att personuppgifter i både öppna, avslutade och arkiverade ärenden undantas från rätten till

radering anser vi att det inte finns något behov av att i utlänningsdatalagen föreskriva ytterligare undantag från denna rättighet.

Avslutningsvis vill vi dock påpeka att vi anser att dataskyddsförordningen inte hindrar myndigheterna att radera personuppgifter som behandlats i strid med gällande personuppgiftsbestämmelser. En förutsättning är dock naturligtvis att detta är tillåtet enligt det övriga regelverk som styr rätten till radering i verksamhetssystemen, t.ex. förvaltningsrättsliga bestämmelser och arkivregler.

### **Rätt att göra invändningar och begära begränsning av behandling**

Den registrerades rätt att enligt artikel 21.1 i dataskyddsförordningen göra invändningar mot att personuppgifter behandlas för myndighetsutövning eller för en uppgift av allmänt intresse, är en utökning jämfört med vad som för närvarande gäller. Som vi tidigare konstaterat anser vi att hela den personuppgiftsbehandling som utförs på utlänningsdatalagens tillämpningsområde sker för att utföra en uppgift av allmänt intresse (se avsnitt 6.3.2). Detta innebär att dataskyddsförordningens bestämmelse om rätten att göra invändningar gäller för den behandling av personuppgifter som utförs i enlighet med utlänningsdatalagen.

Under den tid det tar för myndigheten att efter en registrerads invändning bedöma om skälen för behandlingen väger tyngre än den registrerades skäl mot denna, ska behandlingen begränsas enligt artikel 18.1 d och 18.2 i dataskyddsförordningen. Detsamma gäller, enligt artikel 18.1 a–c i dataskyddsförordningen, under en kontroll av personuppgifternas riktighet, i vissa fall då behandlingen är olaglig eller i vissa fall om uppgifterna inte längre behövs för ändamålen med behandlingen. Den registrerades rätt till begränsning av personuppgiftsbehandling är därmed utförligare än personuppgiftslagens bestämmelser om blockering.

En begränsning innebär enligt huvudregeln i artikel 18.2 att personuppgifter inte får behandlas på något annat sätt än att lagras. Undantag görs dock bl.a. för det fall behandlingen sker av skäl som rör ett viktigt allmänintresse för medlemsstaten.

Att handläggningen av ärenden inom utlänningsdatalagens tillämpningsområde inte avstannar utgör enligt vår mening ett

viktigt allmänintresse. Mot den bakgrunden anser vi att undantaget i artikel 18.2 i dataskyddsförordningen är tillämpligt på de personuppgifter som ingår i pågående ärenden. Följden av detta blir att myndigheternas handläggning av det enskilda ärendet inte behöver avvänta i väntan på att en intresseavvägning ska göras efter en invändning (artikel 18.1 d). Samma resonemang bör enligt vår mening kunna tillämpas vid en invändning om personuppgifternas riktighet (artikel 18.1 a).

Ändamålet med behandlingen av personuppgifter i myndigheternas ärenden är vidare att handlägga just dessa ärenden. Detta borde enligt vår mening medföra att så länge handläggningen av ett ärende inte är avslutad, behövs personuppgifterna för ändamålet med behandlingen. Rätten till begränsning av uppgifter som inte längre behövs för ändamålet (artikel 18.1 c) bör därmed ha mycket liten betydelse för de aktuella myndigheterna vad gäller pågående ärenden. Skulle en sådan situation uppkomma gör vi emellertid även här bedömningen att personuppgifterna fortsatt kan behandlas i öppna ärenden med stöd av undantaget för ett viktigt allmänintresse.

För myndigheterna är det vidare i stor utsträckning de förvaltningsrättsliga regelverken och uppgifter som kommer från den sökande själv som styr vilka personuppgifter som behöver behandlas i ett enskilt ärende. Vi anser därför att en sådan olaglig behandling av personuppgifter där en begränsning av behandling kan krävas (artikel 18.1 b) bör vara mycket sällsynt förekommande.

Vad gäller avslutade ärenden bör bevarande vara tillåtet även om behandlingen av de aktuella personuppgifterna har begränsats, eftersom ett sådant bevarande vanligtvis endast innebär att personuppgifterna lagras. Sökningar bland avslutade ärenden (jfr avsnitt 17.1.4) innebär emellertid en behandling av personuppgifterna utöver lagringen. Sådana sökningar kan exempelvis göras i syftet att återanvända information i ett tidigare ärende vid handläggning av ett nytt ärende gällande samma person. Det utgör enligt vår mening ett viktigt allmänintresse att sådana sökningar får göras vid behov, eftersom det säkerställer en rättssäker ärendehandläggning. Det finns därmed undantag som tillåter att sådan behandling vid behov får fortsätta även om behandlingen av personuppgifter har begränsats i enlighet med artikel 18.1 i dataskyddsförordningen.

Även allmänhetens tillgång till allmänna handlingar utgör enligt vår mening ett viktigt allmänintresse. Detta medför att utlämnande av allmänna handlingar – både i pågående och avslutade ärenden – är tillåtet även om behandlingen av personuppgifter har begränsats. Myndigheternas rätt att lämna ut personuppgifter i allmänna handlingar i enlighet med nationell rätt säkerställs för övrigt även genom artikel 86 i dataskyddsförordningen.

Vi anser sammanfattningsvis att det undantag som finns i artikel 18.2 i dataskyddsförordningen garanterar att myndigheternas handläggning av enskilda ärenden inte avstannar, att bevarande av ärenden är möjlig och att allmänhetens tillgång till allmänna handlingar inte inskränks. Om personuppgifter har behandlats i enlighet med de primära eller sekundära ändamålen i utlänningsdatalagen borde enligt vår mening vidare en sådan intresseavvägning som ska göras enligt artikel 21.1 i dataskyddsförordningen i stort sett uteslutande utfalla till myndighetens fördel. Mot den bakgrunden finns det enligt vår mening inte något egentligt behov av att i utlänningsdatalagen införa ytterligare inskränkningar av rätten att göra invändningar eller rätten att få personuppgiftsbehandlingen begränsad.

Enligt vårt resonemang blir rätten att göra invändningar och rätten att begära att behandlingen begränsas till stora delar illusorisk vad gäller behandling av personuppgifter inom utlänningsdatalagens tillämpningsområde. Man skulle kunna argumentera för att det faktum att den registrerades möjligheter att nå reell framgång med en invändning eller en begäran är ytterst små i en viss verksamhet, innebär att det inte skulle finnas möjlighet att införa ett generellt undantag från dessa rättigheter. Skälet till detta skulle i så fall vara att ett sådant undantag inte är nödvändigt för att säkerställa nationella viktiga mål av generellt allmänt intresse eller något annat av de syften som anges i artikel 23.1 i dataskyddsförordningen. Finns det ingen risk för framgång med en invändning eller en begäran, utgör den inget reellt hot mot exempelvis nationella viktiga mål av allmänt intresse. Vi kan emellertid inte med säkerhet slå fast att det inte finns situationer då det kan finnas grund för en invändning eller en begäran. För att garantera att myndigheternas arbete kan fortsätta ostört, skulle man därför möjligtvis – med stöd av artikel 23.1 i dataskyddsförordningen – kunna föreskriva ett uttryckligt undantag från

rätten enligt artiklarna 18.1 och 21.1 att göra invändningar mot att personuppgifter behandlas och rätten att begära att behandlingen begränsas. Vi stannar emellertid vid bedömningen att en reglering som inskränker de registrerades rättigheter inte bör införas utan sakliga skäl bara för att – sannolikt i ringa omfattning – minska den administrativa bördan med att hantera invändningar eller krav på begränsningar.

Mot denna bakgrund är det vår uppfattning att en bedömning av om behandlingen ska begränsas får göras i varje fall där frågan aktualiseras enligt bestämmelserna i dataskyddsförordningen. Även intresseavvägningen mellan myndighetens skäl för behandlingen och den registrerades skäl mot denna, får enligt vår mening göras varje gång en registrerad gör en invändning mot behandlingen i enlighet med artikel 21 i dataskyddsförordningen. En annan sak är att bedömningen och intresseavvägningen i det stora flertalet fall borde kunna göras relativt standardiserat.

### Underrättelse till mottagarna

Dataskyddsförordningens bestämmelser om underrättelse till mottagarna av personuppgifter vid rättelse, radering eller begränsning av behandling motsvarar vad som, genom en hänvisning till 28 §§ PuL, för närvarande gäller inom utlänningsdatalagens tillämpningsområde. Någon anledning att införa undantag från denna rättighet i utlänningsdatalagen har inte kommit fram.

## 14.7 Automatiserade beslut

Automatiserade beslut blir allt vanligare inom de svenska förvaltningsmyndigheterna.<sup>7</sup> Det finns enligt vår mening därför anledning att i korthet kommentera artikel 22 i dataskyddsförordningen, som reglerar den registrerades rättigheter när det gäller automatiserat beslutsfattande.

---

<sup>7</sup> Jfr förarbetena med förslag till ny förvaltningslag (prop. 2016/17:180 s. 315).

Enligt artikel 22 i dataskyddsförordningen har den registrerade under vissa förutsättningar rätt att inte bli föremål för 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. Profilering innebär, enligt artikel 4.4 i dataskyddsförordningen, 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 personens arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar. Användningen av uttrycket *inbegripet profilering* i artikel 22 är enligt vår mening tvetydigt och innebär att bestämmelsen skulle kunna tolkas som att den avser alla typer av automatiserade beslut. Bestämmelsen i artikel 22 behandlas i skäl 71 till dataskyddsförordningen, som inte heller klargör om uttrycket *inbegripet profilering* är avsett att ses som en exemplifiering eller om det definierar bestämmelsens tillämpningsområde.

I 1995 års dataskyddsdirektiv regleras den registrerades rätt att motsätta sig automatiserat beslutsfattande i artikel 15, som i svensk rätt har genomförts genom 29 § PUL. Dessa två bestämmelser omfattar endast beslut som grundas på automatiserad behandling av sådana personuppgifter som är avsedda att bedöma egenskaper hos personen, dvs. så kallad profilering. Om avsikten vore att artikel 22 i dataskyddsförordningen skulle träffa alla typer av automatiserade beslut och således ha ett vidare tillämpningsområde än motsvarande bestämmelse i 1995 års dataskyddsdirektiv, borde detta enligt vår mening rimligtvis framgå av skälen till förordningen. I skäl 73 till dataskyddsförordningen, som behandlar rätten att i enlighet med artikel 23 i förordningen begränsa den registrerades rättigheter, nämns vidare endast *profileringsbaserade beslut*. Mot den bakgrunden bedömer vi att artikel 22 i dataskyddsförordningen endast är tillämplig för sådana automatiserade beslut som innebär att personuppgifter används för att bedöma personliga egenskaper hos en fysisk person och således innefattar profilering. Bestämmelsen i artikel 22 sätter därmed inga hinder för automatiserade beslut som inte innefattar profilering. Eftersom utlänningsdatalagen varken innehåller någon hänvisning till 29 §

PuL eller några uttryckliga bestämmelser om automatiserat beslutsfattande, åligger det de enskilda myndigheterna att ta ställning till om dataskyddsförordningen föranleder någon förändring vad gäller det automatiserade beslutsfattande som eventuellt förekommer inom myndigheterna.

## **14.8 Skadestånd**

### **14.8.1 Utlänningsdatalagen och personuppgiftslagen**

Enligt artikel 22 i 1995 års dataskyddsdirektiv ska medlemsstaterna 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 ifrågavarande behandling. Direktivet har i denna del genomförts i svensk rätt genom 48 § PuL. Utlänningsdatalagen hänvisar, genom 8 § 12, till denna bestämmelse.

Enligt 48 § PuL ska den personuppgiftsansvarige ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med personuppgiftslagen har orsakat.

### **14.8.2 Dataskyddsförordningen**

Enligt artikel 79.1 i dataskyddsförordningen har alla registrerade rätt till ett effektivt rättsmedel om de anser att deras rättigheter enligt förordningen har åsidosatts som en följd av att deras personuppgifter har behandlats på ett sätt som inte är förenligt med förordningen. Enligt bestämmelsen gäller detta utöver rätten att lämna in ett klagomål till tillsynsmyndigheten. Om den personuppgiftsansvarige – eller personuppgiftsbiträdet – är en myndighet som agerar inom ramen för sin myndighetsutövning ska sådan talan, enligt artikel 79.2 i dataskyddsförordningen, väckas vid domstolarna i den medlemsstat där den personuppgiftsansvarige, eller personuppgiftsbiträdet, är etablerad.

Enligt artikel 82 i dataskyddsförordningen har varje person som lidit materiell eller immateriell skada till följd av en överträdelse av förordningen rätt till ersättning från den personuppgiftsansvarige



eller personuppgiftsbiträdet för den uppkomna skadan. Enligt bestämmelsen är ansvaret solidariskt om flera personuppgiftsansvariga eller personuppgiftsbiträden har medverkat vid samma behandling. Det finns även en uttrycklig regressrätt mellan de ansvariga i en sådan situation. Den personuppgiftsansvarige – eller personuppgiftsbiträdet – ska dock undgå ansvar om denne visar att den inte på något sätt är ansvarig för den händelse som orsakat skadan.

I skäl 146 till dataskyddsförordningen förtydligas att behandling som strider mot dataskyddsförordningen även omfattar bl.a. behandling som strider mot medlemsstaternas nationella rätt med närmare specifikation av förordningens bestämmelser. Detta innebär enligt vår mening att även överträdelse av bestämmelser i de registerförfattningar som behålls eller införs i svensk rätt med stöd av artikel 6.2 och 6.3 i dataskyddsförordningen (se kapitel 5) omfattas av förordningens bestämmelse om skadeståndsansvar.<sup>8</sup>

### 14.8.3 Dataskyddslagen

Dataskyddsutredningen har i sitt betänkande föreslagit att dataskyddslagen ska innehålla en bestämmelse som innebär att rätten till ersättning enligt artikel 82 i dataskyddsförordningen även gäller vid överträdelse av bestämmelser i dataskyddslagen och andra författningar som kompletterar dataskyddsförordningen. Bestämmelsen beskrivs i Dataskyddsutredningens betänkande (SOU 2017:39 s. 304) som en upplysningsbestämmelse och finns i förslaget till 8 kap. 1 § dataskyddslagen.

### 14.8.4 Bedömning

**Förslag:** Rätten till ersättning enligt artikel 82 i dataskyddsförordningen ska gälla även vid överträdelse av bestämmelser i dataskyddslagen och utlänningsdatalagen med tillhörande föreskrifter. Regleringen ska genomföras genom en hänvisning till den föreslagna 8 kap. 1 § dataskyddslagen.

<sup>8</sup> Se även Dataskyddsutredningens betänkande (SOU 2017:39 s. 304 f.).

Vid genomförandet av 1995 års dataskyddsdirektiv bedömde man att personuppgiftslagens skadeståndsbestämmelse – tillsammans med tillsynsmyndighetens möjlighet till vitesföreläggande – utgjorde en effektiv och tillräcklig sanktion.<sup>9</sup> Dataskyddsutredningen har i sitt betänkande (SOU 2017:39 s. 304) gjort bedömningen 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.

Som nämnts ovan kommer, enligt vår bedömning, dataskyddsförordningens bestämmelser om skadestånd även utan hänvisning till förordningen att gälla även för överträdelse av utlänningsdatalagens bestämmelser. Det framgår enligt vår mening dock inte tydligt av artikel 82 i dataskyddsförordningen att skadeståndsansvaret även omfattar överträdelser av de nationella registerförfattningarnas bestämmelser. Vi anser därför att det finns anledning att göra en hänvisning i utlänningsdatalagen till den föreslagna 8 kap. 1 § dataskyddslagen om skadestånd. På detta sätt kommer det att stå fullständigt klart att dataskyddsförordningens bestämmelser om skadestånd gäller även vid överträdelser av utlänningsdatalagstiftningens bestämmelser.

## 14.9 Information om personuppgiftsincidenter

### 14.9.1 Dataskyddsförordningen

Om en personuppgiftsincident sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om incidenten. Detta framgår av artikel 34.1 i dataskyddsförordningen. I artikel 34.3 a–c finns undantag från den personuppgiftsansvariges skyldighet att lämna sådan information till den registrerade. Information behöver inte lämnas om den personuppgiftsansvarige har vidtagit lämpliga tekniska och organisatoriska skyddsåtgärder (led a), om den personuppgiftsansvarige har vidtagit ytterligare

---

<sup>9</sup> Prop. 1997/98:44 s. 107.

åtgärder som innebär att det inte längre uppstår hög risk för de registrerades rättigheter och friheter (led b) eller om det skulle innebära en oproportionerlig ansträngning att lämna sådan information (led c). För det fall undantag enligt led c blir aktuellt ska allmänheten i stället informeras eller så ska en liknande åtgärd vidtas.

### 14.9.2 Bedömning

**Förslag:** Den registrerades rätt att få information om en personuppgiftsincident enligt artikel 34 i dataskyddsförordningen ska inte gälla om den personuppgiftsansvarige, enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning, inte får lämna ut uppgifter till den registrerade.

Den personuppgiftsansvariges skyldighet att, enligt artikel 34 i dataskyddsförordningen, informera den registrerade om en inträffad personuppgiftsincident innebär en utökning jämfört med vad som för närvarande gäller. De befintliga undantagen i artikel 34.3 i dataskyddsförordningen innefattar inte situationer där det råder sekretess eller tystnadsplikt för vissa personuppgifter. Dataskyddsförordningens bestämmelse om information till den registrerade vid en personuppgiftsincident skulle därmed kunna innebära att den registrerade indirekt får information om att hans eller hennes personuppgifter behandlas av Migrationsverket, Polismyndigheten eller utlandsmyndigheterna, trots att det råder sekretess om detta förhållande gentemot den registrerade själv.

Det är inte helt enkelt att ge exempel på en sådan situation. Ett tänkbart scenario är om personen A söker asyl i Sverige och uppger förföljelse från sin make B. Senare söker också B asyl i Sverige, omedvetande om att även A sökt asyl här. Vid en incident som berör A:s ärende skulle B, utan den reglering vi föreslagit, ha rätt att få information om incidenten och därmed indirekt om att A befinner sig i Sverige.

Mot den bakgrunden föreslår vi att det i utlänningsdatalagen införs en bestämmelse med innebörden att bestämmelserna om den registrerades rätt att få information om en personuppgiftsincident enligt artikel 34 i dataskyddsförordningen inte gäller om den

personuppgiftsansvarige, enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning, inte får lämna ut uppgifter till den registrerade. På detta sätt kommer nationella bestämmelser om sekretess eller tystnadsplikt att gå före den registrerades rätt att få information om inträffade incidenter.

Vi anser att ett sådant undantag kan göras med stöd av artikel 23.1 f i dataskyddsförordningen; har en sekretessbestämmelse införts i svensk rätt får det förutsättas att den tillkommit för att säkerställa ett viktigt mål av generellt allmänt intresse eller skyddet för rättsliga åtgärder. Begränsningen bör även vara nödvändig för att skydda de intressen som kommer till uttryck i de nationella sekretessbestämmelserna och utgöra en rimlig avvägning mellan dessa intressen och de registrerades intresse av skydd för den personliga integriteten. Begränsningen sker därmed, enligt vår mening, med respekt för andemeningen i de grundläggande rättigheter och friheter som kommer till uttryck i stadgan (se avsnitt 3.4.1).

Den föreslagna lydelsen motsvarar den reglering som Data-skyddsutredningen har föreslagit för 5 kap. 1 § dataskyddslagen, där undantag från rätten att få information om och tillgång till personuppgifter enligt artiklarna 13–15 i dataskyddsförordningen regleras (se avsnitt 14.3.3). En sådan ordning skulle vidare motsvara det som enligt Utredningen om 2016 års dataskyddsdirektivs förslag till 3 kap. 11 § brottsdatalagen ska gälla i motsvarande situation i den verksamhet som styrs av 2016 års dataskyddsdirektiv.<sup>10</sup>

---

<sup>10</sup> Se Utredningen om 2016 års dataskyddsdirektivs delbetänkande (SOU 2017:29).

# 15 Direktåtkomst och sekretessbrytande bestämmelser

## 15.1 Direktåtkomst

### 15.1.1 Proportionalitetsbedömning

Direktåtkomst är ett sätt att elektroniskt lämna ut uppgifter. I den mån utlämnandet innefattar personuppgifter utgör det en behandling av personuppgifter i dataskyddsförordningens mening.

Dataskyddsförordningen saknar, liksom 1995 års dataskyddsdirektiv, särskilda bestämmelser om elektroniskt utlämnande. Upplivsingsvis kan sägas att skäl 31 till dataskyddsförordningen innehåller en skrivning om att ”offentliga myndigheters begäranden om att uppgifter ska lämnas ut alltid ska vara skriftliga och motiverade, läggas fram i enskilda fall och inte gälla hela register eller leda till att register kopplas samman”. Tagen ur sitt sammanhang skulle skrivningen kunna tolkas som ett hinder mot att etablera direktåtkomst mellan myndigheter. Den förekommer dock i samband med ett resonemang om vem som definitionsmässigt ska betraktas som mottagare av personuppgifter i dataskyddsförordningens mening och – indirekt – om möjligheten att göra undantag från viss informationsskyldighet gentemot registrerade.<sup>1</sup> Vi anser inte att skrivningen ska ges någon betydelse utanför detta mycket begränsade sammanhang.<sup>2</sup>

Enligt artikel 24.1 och artikel 32 i dataskyddsförordningen ska den personuppgiftsansvarige dock genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa att behandlingen

---

<sup>1</sup> Jfr artikel 4.9 samt 13.1 e, 14.1 e, 15.1 c och 30.1 d i dataskyddsförordningen.

<sup>2</sup> Motsatt uppfattning har redovisats i eSamverkansprogrammets vägledning ”Elektroniskt informationsutbyte – en vägledning för utlämnande i elektronisk form” s. 22.

utförs i enlighet med förordningen och att en lämplig säkerhetsnivå säkerställs. Enligt artikel 5.1 a i dataskyddsförordningen måste en personuppgiftsbehandling vidare alltid vara korrekt (skälig och rimlig) i förhållande till den registrerade. För att säkerställa att behandlingen av en personuppgift är skälig i förhållande till den registrerade ska det för varje behandling göras en proportionalitetsbedömning. I den bedömningen vägs behovet av den konkreta behandlingen mot den registrerades intresse av personlig integritet. En behandling av personuppgifter som innebär risker för den personliga integriteten får då genomföras endast om fördelarna med behandlingen står i rimlig proportion till riskerna. Säkerhetsåtgärder som minskar riskerna för den personliga integriteten har här stor betydelse.<sup>3</sup>

Rent allmänt kan nämnas att ett elektroniskt utlämnande av uppgifter bör medföra en större risk för otillbörliga integritetsintrång, eftersom det ger en större möjlighet att bearbeta och sprida informationen jämfört med ett utlämnande som sker i pappersform.<sup>4</sup> Detta måste beaktas i den proportionalitetsbedömning som ska göras.

### 15.1.2 Innebörden av direktåtkomst

Direktåtkomst innebär att uppgifter, däribland personuppgifter, elektroniskt görs tillgängliga för en mottagare utanför myndigheten. Högsta förvaltningsdomstolen ansåg i rättsfallet HFD 2015 ref. 61 att det avgörande för om en direktåtkomst kan anses föreliggande är om upptagningen redan i och med möjligheten att ta del av den kan anses förvarad hos den mottagande myndigheten i den mening som avses i 2 kap. 3 § TF. Enligt denna bestämmelse är så fallet 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.

---

<sup>3</sup> Samma krav gäller enligt artikel 8 i Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, Europarådets konvention om skydd för enskilda vid automatiska databehandling av personuppgifter, nr 108, samt artikel 7 och 8 i EU:s stadga om de grundläggande rättigheterna (2010/C 83/02), jfr Datainspektionen Vägledning för integritetsanalys, september 2016 och Integritetsskyddskommitténs betänkande (SOU 2007:22 s. 449 f.).

<sup>4</sup> Jfr departementspromemorian med förslag till domstolsdatalog (Ds 2013:10 s. 119 f.).

Informationshanteringsutredningen har i sitt betänkande med förslag till ny myndighetsdatalog gjort följande sammanfattning av begreppet direktåtkomst (SOU 2015:39 s. 121 ff.).

Med direktåtkomst avses vanligtvis att någon har direkt tillgång till någon annans register eller databas och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i registret eller databasen (se bl.a. prop. 2009/10:85 s. 168). I begreppet ligger också att den som är personuppgiftsansvarig för registret eller databasen inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst söktillfälle tar del av (prop. 2011/12:45 s. 133). Den myndighet som lämnar ut uppgifter genom direktåtkomst fattar således inte något beslut om utlämnande av de uppgifter som den som har direktåtkomst tar del av i varje enskilt fall. I förarbetena till 11 kap. 4 § OSL, som alltså reglerar överföring av sekretess vid direktåtkomst, uttalade sig regeringen om hur direktåtkomst bör definieras (prop. 2007/08:160 s. 164). Med en sådan åtkomst avsågs enligt regeringen att en upptagning är tillgänglig hos den mottagande myndigheten på ett sådant sätt som avses i 2 kap. 3 § andra stycket första meningen TF, dvs. upptagningen ska vara tillgänglig med tekniska hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas. /.../ Den omständigheten att direktåtkomst till en viss mängd uppgifter innebär att de handlingar i vilka uppgifterna ingår anses expedierade till den mottagande myndigheten medför alltså i sin tur att handlingarna är att anse som förvarade, och därmed också som huvudregel som inkomna, hos den myndigheten i den mening som avses i 2 kap. 3 och 6 §§ TF. Handlingarna utgör genom direktåtkomsten således allmänna handlingar även hos den mottagande myndigheten. En direktåtkomst till sekretessreglerade uppgifter innebär vidare att det krävs en sekretessbrytande regel för att utlämnandet av uppgifterna inte ska innebära ett brott mot den sekretess som annars gäller.

Direktåtkomst innebär således ett elektroniskt utlämnande, som kan omfatta bland annat personuppgifter. Jämfört med ett elektroniskt utlämnande av uppgifter som sker efter en ”manuell” förfrågan är direktåtkomsten emellertid mycket mer omfattande. Den mottagande myndigheten tillåts ju söka fritt i den informationssamling som direktåtkomsten avser och samtliga handlingar som omfattas av direktåtkomsten anses ha expedierats i samma ögonblick som direktåtkomsten upprättas.<sup>5</sup>

Integritetsriskerna med direktåtkomst består således i att den mottagande myndigheten på egen hand får söka bland all

---

<sup>5</sup> Jfr Informationshanteringsutredningens betänkande (SOU 2015:39 s. 136).

information som finns i den aktuella informationssamlingen utan att den utlämnande myndigheten har kontroll över vilka uppgifter som mottagaren tar del av. Direktåtkomsten kan också ge möjlighet för personal på den mottagande myndigheten att hämta hem informationen till sitt eget system och bearbeta den där.<sup>6</sup> Vidare innebär direktåtkomst att den mottagande myndigheten kan vara skyldig att i enlighet med offentlighetsprincipen lämna ut de personuppgifter som omfattas av direktåtkomsten. Givetvis gäller detta med den begränsning som föreskrivs i offentlighets- och sekretesslagen.

Det bör vidare nämnas att offentlighetsprincipen också omfattar uppgifter som ännu inte sammanställts hos en myndighet, men som kan sammanställas med hjälp av tillgänglig teknik och rutinbetonade åtgärder. En sökning är ett exempel på en sådan rutinbetonad åtgärd. Om direktåtkomst tillåter den mottagande myndigheten att göra en viss sökning i värmyndighetens databas och den mottagande myndigheten har fått en begäran om att lämna ut en sammanställning av åtkomliga uppgifter i enlighet med tryckfrihetsförordningen, måste den mottagande myndigheten således göra en sökning och – om hinder inte möter på grund av sekretess – lämna ut de uppgifter sökningen resulterar i.

### 15.1.3 Utlänningsdatalagen och utlänningsdataförordningen

Den yttre ramen för den direktåtkomst som är tillåten inom utlänningsdatalagens tillämpningsområde framgår av 19 § utlänningsdatalagen.<sup>7</sup> Bestämmelsens första stycke innebär att endast Polismyndigheten, Säkerhetspolisen, utlandsmyndigheterna, Försäkringskassan, Pensionsmyndigheten, Skatteverket eller en part eller en parts ombud eller biträde får medges direktåtkomst till personuppgifter hos Migrationsverket. Direktåtkomst för en part eller dess ombud eller biträde får, enligt bestämmelsens andra stycke, endast avse personuppgifter i partens ärende. För att göra utlänningsdatalagen ändamålsenlig över tid har regeringen, enligt 19 § tredje stycket, möjlighet att meddela ytterligare föreskrifter

---

<sup>6</sup> Jfr prop. 2007/08:160 s. 56.

<sup>7</sup> Se förarbetena till utlänningsdatalagen (prop. 2015/16:65 s 91).



om begränsningar av direktåtkomst och om behörighet och säkerhet vid sådan åtkomst.<sup>8</sup> Regeringen har även möjlighet att vidaredelegera föreskriftsrätten till myndighet i denna del.

Regeringen har utnyttjat sin föreskriftsrätt genom att i 8–13 §§ utlänningsdataförordningen uttömmande reglera i vilka fall direktåtkomst får medges samt vilka personuppgifter som får omfattas av sådan åtkomst. Regleringen innebär sammanfattningsvis att Polismyndighetens och utlandsmyndigheternas direktåtkomst endast får avse de personuppgifter som dessa myndigheter behöver för att utföra vissa verksamheter som beskrivs i utlänningsdatalagens ändamålsbestämmelser (9 respektive 10 §§ utlänningsdataförordningen). Säkerhetspolisens direktåtkomst ska begränsas till de personuppgifter som myndigheten behöver för att fullgöra sina uppgifter enligt utlänningslagen (2005:716), lagen (1991:527) om särskild utlänningskontroll och lagen (2001:82) om svenskt medborgarskap (11 § utlänningsdatalagen).

Försäkringskassans, Pensionsmyndighetens och Skatteverkets direktåtkomst är begränsad till de uppgifter myndigheterna behöver i viss utpekad verksamhet eller för handläggning av vissa utpekade ärenden. Den får därtill endast avse vissa specifikt uppräknade kategorier av personuppgifter (12 och 13 §§ utlänningsdataförordningen).

Utlänningsdataförordningens bestämmelser om direktåtkomst innebär att en part eller dess ombud eller biträde för närvarande inte får medges direktåtkomst (19 § utlänningsdatalagen jämförd med 8 § utlänningsdataförordningen).

Enligt 14 § utlänningsdataförordningen får Migrationsverket meddela ytterligare föreskrifter om begränsningar av möjligheterna att lämna ut personuppgifter genom direktåtkomst. Verket får enligt samma bestämmelse även meddela föreskrifter om behörighets- och säkerhetskrav för att direktåtkomst till personuppgifter hos Migrationsverket ska få medges de myndigheter som anges i 19 § utlänningsdatalagen. Enligt vad vi erfarit finns det för närvarande inte några sådana föreskrifter. Av 14 § utlänningsdataförordningen framgår även att direktåtkomst inte får medges innan Migrationsverket har försäkrat sig om att den mottagande myndigheten uppfyller uppställda krav på behörighet och säkerhet.

---

<sup>8</sup> Se förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 91).

## 15.2 Sekretessbrytande bestämmelser

Bestämmelser om direktåtkomst anses inte ha någon sekretessbrytande verkan.<sup>9</sup> Därför finns i 20 § första stycket utlänningsdatalagen en sekretessbrytande bestämmelse som träffar Polismyndighetens, Säkerhetspolisens och utlandsmyndigheternas direktåtkomst till de personuppgifter som Migrationsverket behandlar.<sup>10</sup> Bestämmelsen innebär att de tre myndigheterna har rätt att ta del av de personuppgifter om enskilda som Migrationsverket behandlar med stöd av samtliga primära ändamål i 11 § utlänningsdatalagen. Polismyndigheten har därutöver rätt att få tillgång till uppgifter som Migrationsverket enligt 14 § utlänningsdatalagen behandlar i sina register över fingeravtryck och fotografier.

I 20 § andra och tredje stycket utlänningsdatalagen finns sekretessbrytande bestämmelser som tar sikte på Migrationsverkets uppgiftslämnande i enskilda fall – t.ex via telefon eller e-post – till Polismyndigheten, Säkerhetspolisen eller en utlandsmyndighet.<sup>11</sup>

## 15.3 Bedömning

**Förslag:** Dataskyddsförordningen föranleder ingen ändring i sak av utlänningsdatalagens och utlänningsdataförordningens bestämmelser om direktåtkomst. Detsamma gäller för de sekretessbrytande bestämmelser som finns i utlänningsdatalagen.

Om direktåtkomst innefattar personuppgifter innebär den också en behandling av sådana uppgifter. För den avsändande myndigheten består behandlingen av att den lämnar ut personuppgifter och för den mottagande myndigheten av att den samlar in dem.

Direktåtkomst regleras inte uttryckligen i vare sig 1995 års dataskyddsdirektiv eller i dataskyddsförordningen. Precis som

<sup>9</sup> Se b.l.a. förarbetena till lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet (prop. 2004/05:164 s. 83).

<sup>10</sup> Sekretessbrytande bestämmelser som träffar Försäkringskassans, Pensionsmyndighetens och Skatteverkets direktåtkomst finns i annan lagstiftning (se förarbetena till utlänningsdatalagen, prop. 2015/16:65 s. 93).

<sup>11</sup> Se förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 93 f.).

enligt 1995 års dataskyddsdirektiv är dock en av grundprinciperna för personuppgiftsbehandlingen enligt dataskyddsförordningen att behandlingen ska vara korrekt i förhållande till den registrerade. Korrektheten innefattar att behandlingen ska vara rimlig eller skäligen. Vid bedömningen av om direktåtkomst mellan myndigheter är förenlig med dataskyddsförordningen måste man således göra en avvägning mellan de effektivitetsvinster och andra fördelar som direktåtkomst medför för de inblandade myndigheterna och parterna och de risker den innebär för den enskildes integritet. För att direktåtkomst ska vara tillåten måste det efter en sådan proportionalitetsbedömning konstateras att fördelarna med behandlingen står i rimlig proportion till riskerna. Av betydelse är också vilka säkerhetsåtgärder som kan vidtas för att minska riskerna för den personliga integriteten.

Dataskyddsförordningens krav på proportionalitet är inte något nytt. Samma principer gällde enligt 1995 års dataskyddsdirektiv. Vid tillkomsten av utlänningsdatalagen måste lagstiftaren därför ha gjort bedömningen att fördelarna med den direktåtkomst som tillåts enligt lagen och tillhörande förordning står i rimlig proportion till riskerna.

Vad gäller integritetsriskerna kan sägas att det är oundvikligt att direktåtkomst till de uppgifter som finns i Migrationsverkets ärendehanteringssystem avser ett stort antal fysiska personers personuppgifter. Det ligger vidare i verksamhetens natur att de personuppgifter som behandlas till stor del är av ett känsligt slag.

Direktåtkomst för Polismyndigheten och utlandsmyndigheten får endast omfatta sådana personuppgifter som myndigheterna behöver för verksamhet inom utlänningsdatalagens tillämpningsområde. Samma regler för behandlingen av personuppgifter kommer därmed att gälla för den mottagande myndigheten som för "värdmyndigheten" i dessa fall, eftersom de båda omfattas av utlänningsdatalagen och utlänningsdataförordningen. Detta innebär att det skydd i form av ändamålsbegränsningar, behörighetsbegränsningar och sökbegränsningar som finns för personuppgifterna hos Migrationsverket även finns hos den mottagande myndigheten. Ändamåls- och behörighetsbegränsningarna säkerställer att tjänstemän på den mottagande myndigheten endast behandlar de personuppgifter som behövs för arbetsuppgifterna. Sökbegränsningarna innebär ett skydd mot att

de anställda på den mottagande myndigheten för egen del gör sökningar som inte är tillåtna. De bidrar dessutom till att de anställda inte får ta fram och sammanställa personuppgifter utifrån de förbjudna sökbegreppen efter begäran från allmänheten, vilket är av minst lika stor betydelse från integritetssynpunkt. Samtliga dessa omständigheter bidrar till att minska integritetsriskerna för den enskilde.

Liknande bestämmelser finns i de registerförfattningar som gäller för personuppgiftsbehandling i Säkerhetspolisens, Försäkringskassans, Pensionsmyndighetens och Skatteverkets verksamheter.<sup>12</sup> Mot denna bakgrund och med hänsyn till att en avsaknad av direktåtkomst rimligtvis skulle innebära stora effektivitets- och rättsäkerhetsförluster, anser även vi att fördelarna med direktåtkomsten överväger de nackdelar i integritetshänseende som den medför. I avsnitt 18.2 gör vi vidare bedömningen att dataskyddsförordningen inte hindrar att nationella bestämmelser om personuppgiftsbehandling införs i en förordning eller i en myndighetsföreskrift, så länge föreskrifterna tillkommit i laga ordning. Någon anledning att på grund av dataskyddsförordningen ändra utlänningsdatalagens och utlänningsdataförordningens bestämmelser om direktåtkomst finns enligt vår mening därmed inte. Det samma gäller de sekretessbrytande bestämmelser som finns i 20 § utlänningsdatalagen. Vi föreslår dock att 14 § utlänningsdatalagen, som reglerar Migrationsverkets register över fingeravtryck och fotografier, i sin helhet ska återfinnas i en ny 15 a § (se avsnitt 12.1.5). Med anledning av detta behöver mindre redaktionella ändringar göras i 20 § utlänningsdatalagen och 9 § utlänningsdataförordningen.

---

<sup>12</sup> Se polisdatalagen (2010:361), lagen (2003:763) om behandling av personuppgifter inom socialförsäkringens administration och lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet. Det är rimligt att anta att ett liknande skydd för den personliga integriteten kommer att finnas kvar även efter den pågående anpassningen av dessa registerförfattningar till EU:s nya dataskyddsreform (se exempelvis Utredningen om 2016 års dataskyddsdirektivs delbetänkande [SOU 2017:29]).

# 16 Tredjelandsoverföringar

## 16.1 Utlänningsdatalagen och personuppgiftslagen

I 8 § första stycket 8 utlänningsdatalagen finns en hänvisning till 33–35 §§ PuL, som gäller överföring av personuppgifter till tredjeland. Av 33 § första stycket PuL framgår att det är förbjudet att föra över personuppgifter som är under behandling till tredjeland om landet inte har en adekvat nivå för skyddet av personuppgifterna. Förbudet gäller också överföring av personuppgifter för behandling i tredjeland. Bestämmelsen i 34 § PuL innehåller undantag från förbudet; överföring av personuppgifter till tredjeland utan adekvat skyddsnivå är t.ex. tillåten om det behövs för fullgörande av vissa avtal eller för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras. I 35 § PuL finns bestämmelser om regeringens föreskrifträtt på området.

I förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 96 ff.) gjorde regeringen bedömningen att personuppgiftslagens bestämmelser om tredjelandsoverföringar inte tillgodoser all sådan överföring av personuppgifter som är befogad inom utlänningsdatalagens tillämpningsområde. Som exempel nämndes att de aktuella myndigheterna kan ha behov av att föra över personuppgifter till exempelvis förtroendeadvokater i tredjeland när utlandsmyndigheter biträder svenska myndigheter med utredning i enskilda ärenden. Vidare nämndes sådana utlämnanden som behövs när Migrationsverket i ärenden om återvändande behöver ordna resehandlingar och mottagande i mottagarlandet. Slutligen behöver Polismyndigheten i verkställighetsärenden ibland kontakta utländska beskickningar för att fastställa en persons identitet eller för att få ut resehandlingar för personen. Regeringen bedömde att det som utgångspunkt är av allmänt intresse att personuppgifter som behandlas enligt utlänningslagstiftningen kan föras över till

tredjeland när det krävs för att de svenska myndigheterna ska kunna utföra sina uppgifter på ett effektivt sätt.

Mot den bakgrunden finns det i 21 § första stycket utlänningsdatalagen en bestämmelse som innebär att det, trots hänvisningen till 33 § PuL, är tillåtet att även utan den registrerades samtycke föra över personuppgifter till tredjeland om överföringen är absolut nödvändig för de ändamål som anges i 11 § 1 och 2 samt 12 § 1 utlänningsdatalagen (handläggning av ärenden eller biträde i sådana ärenden, kontroll av utlämning samt återsökning av rättslig information). En förutsättning är dock att det inte möter hinder av sekretess enligt offentlighets- och sekretesslagen. Regeringen eller den myndighet som regeringen bestämmer kan, enligt 21 § andra stycket utlänningsdatalagen, meddela ytterligare föreskrifter om begränsningar av möjligheten att föra över personuppgifter till tredjeland. Regeringen har utnyttjat denna möjlighet genom att i 15 § utlänningsdataförordningen föreskriva att personuppgifter som behandlas för återsökning av rättslig information enligt 12 § 1 utlänningsdatalagen (återsökning av rättslig information) får föras över till tredjeland endast om uppgifterna inte direkt pekar ut den registrerade. Utlänningsdatalagens bestämmelser bedömdes i denna del vara förenliga med 1995 års dataskyddsdirektivs bestämmelse om undantag från överföringsförbudet för ett viktigt allmänt intresse (artikel 26.1.d).<sup>1</sup>

## 16.2 Dataskyddsförordningen

Bestämmelser om under vilka förutsättningar personuppgifter får överföras till tredjeland finns i femte kapitlet (artikel 44–49) i dataskyddsförordningen. Bestämmelserna innebär i korthet följande. Överföring av personuppgifter till tredjeland får ske endast om den personuppgiftsansvarige uppfyller villkoren i kapitlet (artikel 44). Personuppgifter får överföras till ett tredjeland om kommissionen har beslutat att landet säkerställer en adekvat skyddsnivå för uppgifterna (artikel 45). Om ett sådant beslut saknas, får personuppgifter endast föras över till tredjeland efter att lämpliga skyddsåtgärder har vidtagits och under förutsättning att

---

<sup>1</sup> Se förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 98).

lagstadgade rättigheter och effektiva rättsmedel finns tillgängliga för de registrerade. De skyddsåtgärder som avses kan bl.a. bestå i rättsligt bindande och verkställbara instrument mellan offentliga myndigheter, bindande företagsbestämmelser eller standardiserade dataskyddsbestämmelser som antagits av kommissionen eller en tillsynsmyndighet (artikel 46). Artikel 47 innehåller närmare bestämmelse om bindande företagsbestämmelser. Artikel 48 reglerar rätten att lämna ut personuppgifter efter domstols- eller myndighetsbeslut från tredjeland.

Om det inte finns något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder får personuppgifter föras över till ett tredjeland endast om vissa villkor, som framgår av artikel 49.1 a–g, är uppfyllda. Det undantag som enligt vår mening främst är aktuellt inom utlänningsdatalagens tillämpningsområde är det som framgår av led d. Enligt denna bestämmelse får överföring av personuppgifter ske till tredjeland om det är nödvändigt av viktiga skäl som rör allmänintresset. Av artikel 49.4 framgår att ett sådant allmänintresse ska vara erkänt i unionsrätten eller i den nationella rätten. Enligt artikel 49.5 får det vidare i medlemsstaternas nationella rätt uttryckligen fastställas gränser för överföringen av specifika kategorier av personuppgifter till ett tredjeland om det saknas beslut om adekvat skyddsnivå. Medlemsstaterna ska underätta kommissionen om sådana bestämmelser.

### 16.3 Bedömning

**Förslag:** Det ska klargöras i utlänningsdatalagen att sådana överföringar av personuppgifter till tredjeland som avses i 21 § första stycket den lagen får ske även om det inte finns något beslut om adekvat skyddsnivå enligt artikel 45.3 eller lämpliga skyddsåtgärder enligt artikel 46 i dataskyddsförordningen.

Bestämmelsen om tredjelandsoverföringar i 21 § utlänningsdatalagen har införts med stöd av undantaget för viktiga allmänna intressen i 1995 års dataskyddsdirektiv. Den bedömning som gjordes i denna del har enligt vår mening alltjämt relevans. De ändamål som omfattas av undantaget i 21 § – handläggning av ärenden inom utlänningsdatalagens tillämpningsområde, kontroll

av utläningar samt återsökning av rättslig information – är vidare erkända i svensk rätt. Överföring till tredjeland kan enligt vår bedömning därmed ske för dessa ändamål med stöd av artikel 49.1 d i dataskyddsförordningen.

Undantagen i artikel 49 förutsätter inte reglering i nationell lagstiftning. De överföringar som omfattas av 21 § utlänningsdatalagen skulle enligt vår mening därmed få utföras även utan reglering i svensk registerförfattning. Vi anser dock att det även fortsättningsvis finns anledning att klargöra att de aktuella tredjelandsoverföringarna är tillåtna. Utlänningsdataförordningens ytterligare inskränkning av rätten att föra över personuppgifter för återsökning av rättslig information (15 §) innebär dessutom att de registrerades integritet skyddas i dessa situationer, vilket är förenligt med dataskyddsförordningens intentioner. Enligt vår bedömning rör det sig vidare om en sådan tillåten specificering av dataskyddsförordningens bestämmelser som medlemsstaterna har rätt att behålla med stöd av artikel 6.2 och 6.3 i dataskyddsförordningen (se kapitel 5). Det bör dock uppmärksammas att undantagen i 21 § utlänningsdatalagen inte kommer att vara uttömmande; artikel 49 i dataskyddsförordningen ska tillämpas för sådana tredjelandsoverföringar som inte omfattas av utlänningsdatalagens och utlänningsdataförordningens bestämmelser. Systematiken stämmer överens med vad som för närvarande gäller i förhållande till undantagen i 34 § PuL.

Eftersom 21 § utlänningsdatalagen hänvisar till personuppgiftslagen måste en justering göras. Vi föreslår att bestämmelsen ska formuleras så att de uppräknade överföringarna ska få göras även om det inte finns något beslut om adekvat skyddsnivå enligt artikel 45.3 eller lämpliga skyddsåtgärder enligt artikel 46 i dataskyddsförordningen. Formuleringen motsvarar de förutsättningar för undantag som framgår av artikel 49.1 i dataskyddsförordningen. För läsbarheten bör enligt vår mening även vissa ytterligare redaktionella ändringar göras. Dessa är emellertid inte avsedda att innebära någon ändring i sak.



# 17 Bevarande, avskiljande och gallring av personuppgifter

## 17.1 Bevarande av personuppgifter

### 17.1.1 Utlänningsdatalagen och personuppgiftslagen

I 8 § första stycket 2 och 3 utlänningsdatalagen finns hänvisningar till 8 och 9 §§ PuL. Delar av de sistnämnda bestämmelserna reglerar förhållandet mellan personuppgiftslagens bestämmelser och rätten att bevara handlingar. I 9 § används begreppen *historiska*, *statistiska* och *vetenskapliga ändamål*. *Historiska ändamål* innefattar här bevarande av handlingar för arkivändamål.<sup>1</sup>

Arkivering av handlingar innebär att de personuppgifter som ingår i handlingarna vidarebehandlas, dvs. behandlas för ett annat ändamål än det ursprungliga. Av 9 § första stycket d PuL framgår att personuppgifter inte får behandlas för ändamål som är oförenliga med det ändamål som uppgifterna samlades in för (finalitetsprincipen). Behandling av personuppgifter för bl.a. historiska ändamål ska, enligt 9 § andra stycket, emellertid inte ses som oförenlig med de ursprungliga ändamålen. Eftersom utlänningsdatalagens primära ändamålsbestämmelser är uttömmande har hänvisningen till 9 § PuL dock inte någon funktion i dessa fall. Endast vad gäller behandling för det sekundära ändamålet att tillhandahålla information (13 §) har finalitetsprincipen betydelse på utlänningsdatalagens tillämpningsområde (se avsnitt 8.2.1).<sup>2</sup>

Enligt 9 § första stycket i PuL är huvudregeln att personuppgifter inte får bevaras längre än vad som är nödvändigt med

---

<sup>1</sup> Jfr förarbetena till personuppgiftslagen (prop. 1997/98:44 s 47 f.).

<sup>2</sup> Jfr 2014 års utlänningsdatautrednings betänkande (SOU 2015:73 s. 265 ff. och s. 434).

hänsyn till det ursprungliga ändamålet. Bestämmelserna i personuppgiftslagen hindrar emellertid inte att myndigheter arkiverar och bevarar handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. I dessa fall ska personuppgiftslagens begränsningar om lagringstid m.m. inte gälla (jfr 8 § andra stycket PuL). Enligt 8 § andra stycket utlänningsdatalagen har emellertid de gallringsbestämmelser som finns i den lagen eller i föreskrifter som har meddelats i anslutning till lagen, företräde före den rätt att arkivera och bevara handlingar som framgår av 8 § andra stycket PuL. Sådana gallringsbestämmelser finns för närvarande för Migrationsverkets register över fingeravtryck och fotografier i 3 § utlänningsdataförordningen. Dessa bestämmelser behandlas närmare i avsnitt 17.3.

För personuppgifter som behandlas för arkivändamål finns, enligt 9 § fjärde stycket PuL, vissa begränsningar för hur uppgifterna får användas. Sådana uppgifter får inte användas för att vidta åtgärder i fråga om den registrerade, om det inte görs med samtycke eller det annars finns synnerliga skäl med hänsyn till den registrerades intressen att göra detta. I 8 § andra stycket PuL finns dock ett undantag, som innebär att myndigheter får använda information i allmänna handlingar för att t.ex. vidta åtgärder beträffande enskilda. Bakgrunden till det aktuella undantaget har i doktrinen i första hand bedömts vara att myndigheternas arkiv enligt 3 § tredje stycket arkivlagen (1990:782) ska tillgodose bl.a. behovet av information för rättskipningen och förvaltningen.<sup>3</sup>

Av 9 § första stycket i PuL framgår att personuppgifter inte får bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Enligt 9 § tredje stycket får personuppgifter dock bevaras för bl.a. historiska ändamål så länge det behövs för detta ändamål. Det kan i myndigheternas verksamhet även finnas anledning att elektroniskt bevara personuppgifter utan att formellt arkivera dem, t.ex. för att för framtida ärendehantering bevara en föredragningspromemoria från ett specifikt ärende. Av förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 101) framgår sammanfattningsvis följande. Bestämmelserna i 9 § första stycket i och tredje stycket PuL gäller för personuppgifter som inte finns i allmänna handlingar. Av de

---

<sup>3</sup> Öman och Lindblom, Personuppgiftslagen (15 sept 2016, Zeteo), kommentaren till 8 §.

bestämmelserna följer att personuppgifter som huvudregel inte får bevaras under längre tid än vad som är nödvändigt med hänsyn till de ändamål för vilka uppgifterna behandlas. Det medför bland annat att personuppgifter i minnesanteckningar eller utkast till beslut eller skrivelser som behandlas av en tjänsteman i ett ordbehandlingsprogram och som inte har tagits om hand för arkivering, ska tas bort ut systemet eller avidentifieras när de inte längre behövs för sitt ändamål.

Hänvisningarna i utlänningsdatalagen till 8 och 9 §§ PuL innebär således i sammanfattning följande. Myndigheterna får, i enlighet med arkivreglerna, elektroniskt arkivera personuppgifter som samlats in med stöd av de primära ändamålsbestämmelserna i utlänningsdatalagen, oavsett om de före arkiveringstidpunkten förekommer i allmänna eller icke allmänna handlingar. De personuppgifter som har arkiverats får användas för att vidta åtgärder i fråga om den registrerade. För personuppgifter som bevaras utan att arkiveras (t.ex. i föredragningspromemorior) gäller att de får behandlas så länge det är nödvändigt för det ändamål de samlades in för.

### 17.1.2 Dataskyddsförordningen

Vidarebehandling av personuppgifter får, enligt artikel 5.1 b i dataskyddsförordningen, ske endast om den är förenlig med de ändamål som personuppgifterna samlades in för. Av bestämmelsen framgår dock att vidarebehandlingen ska anses vara förenlig med de ursprungliga ändamålen när den sker för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1.

Vi bedömer att hänvisningen till artikel 89.1 innebär att arkivering av personuppgifter endast anses förenlig med de ursprungliga ändamålen – och därmed tillåten – om sådana säkerhetsåtgärder som beskrivs i den senare artikeln vidtas. Av artikel 89.1 framgår att behandling av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål samt statistiska ändamål ska omfattas av lämpliga skyddsåtgärder för den registrerades rättigheter och friheter. Det framgår också att dessa skyddsåtgärder ska säkerställa

att det införs sådana tekniska och organisatoriska åtgärder som garanterar att principen om uppgiftsminimering följs. Som exempel nämns att pseudonymisering eller andra åtgärder som innebär att de registrerade inte kan identifieras ska användas när detta är möjligt med hänsyn till arkivändamålet.

Även vad gäller tiden för lagring av personuppgifter har arkiverade uppgifter en särställning i dataskyddsförordningen. Enligt artikel 5.1 e i förordningen får personuppgifter som enbart behandlas för arkivändamål av allmänt intresse lagras i en form som möjliggör identifiering av den registrerade under längre tid än vad som är nödvändigt för de ändamål som de samlades in för. En förutsättning för att så ska få ske är enligt samma bestämmelse att det genomförs lämpliga tekniska och organisatoriska åtgärder för att säkerställa den registrerades rättigheter och friheter.

Även känsliga personuppgifter kan ingå i de handlingar som arkiveras. Dataskyddsförordningens huvudregel är i och för sig att behandling av känsliga personuppgifter är förbjuden (artikel 9.1). Som ett av undantagen anges dock i artikel 9.2 j att behandling av känsliga personuppgifter är tillåten om den är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1. Behandlingen måste då ske 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. Detta innebär enligt vår bedömning i klartext att det krävs stöd i EU-rätten eller i nationell lagstiftning för att känsliga personuppgifter ska få behandlas för bl.a. arkivändamål. Den nationella regleringen måste vidare innehålla säkerhetsåtgärder till skydd för personuppgifterna.

Avslutningsvis vill vi i detta sammanhang nämna att dataskyddsförordningen innehåller vissa undantag från de registrerades rättigheter (tredje kapitlet i förordningen) för de personuppgifter som behandlas för arkivändamål av allmänt intresse. De undantag som är relevanta inom utlänningsdatalagens tillämpningsområde har vi behandlat i kapitel 14.

### 17.1.3 Dataskyddslagen

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39 s. 216) gjort bedömningen 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 för arkivändamål av allmänt intresse. Dataskyddsutredningen menar att det därmed inte krävs någon annan rättslig grund än den med stöd av vilken insamlingen av personuppgifter medgavs för att arkivering av personuppgifter i myndigheters verksamhet ska vara tillåten (jfr artikel 5.1 b i dataskyddsförordningen och skäl 50 till förordningen).

Dataskyddsutredningen har dock föreslagit att dataskyddslagen ska innehålla en bestämmelse som innebär att även känsliga personuppgifter får behandlas för arkivändamål av allmänt intresse, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om bevarande och vård av arkiv. Bestämmelsen finns enligt förslaget i 3 kap. 6 § första stycket dataskyddslagen. Enligt förslaget till andra stycket i samma bestämmelse får regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om att känsliga personuppgifter får behandlas för arkivändamål av allmänt intresse även i andra fall än de som avses i första stycket. Av Dataskyddsutredningens betänkande (SOU 2017:39 s. 223) framgår att bestämmelsen i andra stycket tar sikte på enskilda arkiv som inte omfattas av arkivlagstiftningen. Den är därmed inte av intresse för Migrationsverkets, Polismyndighetens och utlandsmyndigheternas personuppgiftsbehandling.

Dataskyddsutredningen har gjort bedömningen att den svenska lagstiftningen på arkivområdet är proportionell till det eftersträvade syftet och förenlig med det väsentliga innehållet i rätten till dataskydd. I denna bedömning har de skyddsåtgärder som finns i registerförfattningar samt i form av sekretessbestämmelser och gallringsföreskrifter vägt in. De nationella sekretessbestämmelserna bedöms vidare utgöra en särskild skyddsåtgärd, eftersom de har utformats efter en avvägning mellan behovet av skydd och intresset av insyn.<sup>4</sup>

---

<sup>4</sup> Se Dataskyddsutredningens betänkande (SOU 2017:39 s. 221 och 227).

Som en ytterligare skyddsåtgärd för arkiverade personuppgifter har Dataskyddsutredningen föreslagit en bestämmelse i dataskyddslagen (4 kap. 1 §) som motsvarar 8 § andra stycket andra meningen och 9 § fjärde stycket PuL.<sup>5</sup> Enligt den föreslagna bestämmelsen får personuppgifter som behandlas enbart för arkivändamål av allmänt intresse 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. Av bestämmelsen andra stycke framgår att begränsningen inte hindrar myndigheter från att använda personuppgifter som finns i allmänna handlingar.

Dataskyddsutredningen har därutöver föreslagit att dataskyddslagen ska innehålla en bestämmelse som innebär att behandling av personuppgifter om fällande domar i brottmål, lagöverträdelser som innefattar brott eller straffprocessuella tvångsmedel får behandlas om det är nödvändigt för att den personuppgiftsansvarige ska kunna följa föreskrifter om bevarande och vård av arkiv (3 kap. 11 §). Vi anser att denna bestämmelse inte är relevant inom utlänningsdatalagens tillämpningsområde. Anledningen till detta är att sådana uppgifter enligt artikel 10 i dataskyddsförordningen får behandlas av myndigheter. Artikel 10 innehåller inga begränsningar, vilket enligt vår mening måste innebära att detta gäller även när uppgifterna behandlas för arkivändamål.

#### 17.1.4 Bedömning

**Förslag:** Personuppgifter som behandlas eller har behandlats för utlänningsdatalagens primära ändamål ska också få behandlas om det behövs för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 i dataskyddsförordningen.

Känsliga personuppgifter ska inom utlänningsdatalagens tillämpningsområde få behandlas för arkivändamål av allmänt intresse om behandlingen är nödvändig för att en myndighet ska kunna följa föreskrifter om bevarande och vård av arkiv. Regleringen ska genomföras genom en hänvisning i utlännings-

<sup>5</sup> A.a. s. 222.

datalagen till den föreslagna 3 kap. 6 § första stycket dataskyddslagen.

Det ska även fortsättningsvis vara möjligt för Migrationsverket, Polismyndigheten och utlandsmyndigheterna att återanvända personuppgifter i arkiverade mål och ärenden. Regleringen ska genomföras genom en hänvisning i utlänningsdatalagen till den föreslagna 4 kap. 1 § dataskyddslagen.

## Begreppet arkivändamål av allmänt intresse

I samtliga dataskyddsförordningens bestämmelser som rör bevarande av personuppgifter används begreppet *arkivändamål av allmänt intresse* för att beskriva de ändamål för behandling som träffas av bestämmelserna. Vi har tidigare gjort bedömningen att ett utlämnande av personuppgifter enligt tryckfrihetsförordningen utgör en uppgift av allmänt intresse (avsnitt 6.3.2). Bevarandet av allmänna handlingar är en förutsättning för att allmänheten, genom offentlighetsprincipen, ska få fullgod insyn i myndigheternas verksamhet. Redan i förarbetena till personuppgiftslagen gjorde också regeringen bedömningen att ett bevarande av allmänna handlingar utgör en arbetsuppgift av allmänt intresse.<sup>6</sup> Mot den bakgrunden delar vi Dataskyddsutredningens bedömning att den behandling av personuppgifter som myndigheter och andra organ utför när de arkiverar handlingar enligt gällande arkivlagstiftning, sker för arkivändamål av allmänt intresse. Detta innebär att dataskyddsförordningens begrepp *arkivändamål av allmänt intresse* innefattar den arkivering av handlingar som utförs i myndigheternas verksamhet.

Vi anser dock att det endast är de personuppgifter som finns i handlingar som är avsedda att officiellt tas om hand för arkivering som kan anses behandlas för *arkivändamål av allmänt intresse*. Begreppet omfattar således inte sådant elektroniskt bevarande av personuppgifter som inte sker i arkiveringssyfte.

Detta innebär enligt vår mening att ett elektroniskt bevarande av exempelvis en föredragningspromemoria eller en rättsutredning som innehåller personuppgifter – och som inte formellt arkiveras –

---

<sup>6</sup> Prop. 1997/98:44 s. 47.

måste ske enligt de vanliga reglerna i dataskyddsförordningen och utlänningsdatalagen.

### **Arkivering omfattas av utlänningsdatalagens tillämpningsområde**

Genom arkivering tas handlingar från en myndighets kärnverksamhet om hand och bevaras, antingen av myndigheten själv eller av en arkivmyndighet. Enligt huvudregeln får informationen i dessa handlingar under vissa förutsättningar fortfarande användas för att vidta åtgärder beträffande enskilda, trots att arkivering har skett (8 § andra stycket PuL). Detta gäller även på utlänningsdatalagens tillämpningsområde (8 § första stycket 2 utlänningsdatalagen). Enligt förslaget i Dataskyddsutredningens betänkande (SOU 2017:39) ska dataskyddslagen innehålla motsvarande bestämmelser.

För oss är det en självklarhet att personuppgifter som härrör från en myndighets kärnverksamhet fortsätter vara en del av denna verksamhet även efter det att handlingarna de ingår i har arkiverats, åtminstone så länge arkiveringen sker hos myndigheten själv. När handlingarna lämnas över till en arkivmyndighet och inte längre finns kvar hos Migrationsverket, Polismyndigheten eller utlandsmyndigheterna torde utlänningsdatalagen inte heller längre vara tillämplig, eftersom myndigheterna då inte själva behandlar personuppgifterna i handlingarna.

Att arkivering av personuppgifter som härrör från de verksamheter som omfattas av utlänningsdatalagen faller under lagens tillämpningsområde förefaller också vara utgångspunkten i de tidigare förarbetena till lagen. Utlänningsdatalagen gäller för Migrationsverkets, Polismyndighetens och utlandsmyndigheternas personuppgiftsbehandling i de verksamheter som framgår av 2 och 3 §§. För det fall lagstiftaren hade ansett att arkiverade handlingar inte längre utgör en del av dessa verksamheter skulle en hänvisning till personuppgiftslagens bestämmelser om rätten för myndigheter att arkivera allmänna handlingar inte fyllt någon funktion.



## Komplettering av ändamålsbestämmelserna

Enligt utlänningsdatalagens ändamålsbestämmelser får personuppgifter behandlas för att utföra vissa generellt angivna arbetsuppgifter (11 och 12 §§). Personuppgifter som behandlats för dessa ändamål får även behandlas om det är nödvändigt för att tillhandahålla information i vissa fall (13 §).

Arkivering av personuppgifter omfattas enligt vår mening inte av utlänningsdatalagens ändamålsbestämmelser. Genom hänvisningen till 8 § andra stycket PuL klargörs emellertid att arkivering av personuppgifter inom utlänningsdatalagens tillämpningsområde ändå får ske. Dataskyddslagen kommer enligt Dataskyddsutredningens förslag inte att innehålla någon bestämmelse som motsvarar 8 § andra stycket PuL.<sup>7</sup> Anledningen till detta är, som vi förstått det, att det framgår av artikel 5.1 b i dataskyddsförordningen att vidarebehandling av personuppgifter för bl.a. arkivändamål av allmänt intresse ska anses vara förenlig med de ursprungliga ändamålen.<sup>8</sup>

Utlänningsdatalagens primära ändamålsbestämmelser är emellertid avsedda att vara uttömmande, vilket innebär att det för primära ändamål aldrig blir aktuellt för myndigheterna att bedöma om behandling för andra ändamål är förenligt med finalitetsprincipen. Den möjlighet som finns att vidarebehandla insamlade personuppgifter i enlighet med finalitetsprincipen omfattar vidare endast tillhandahållande av information och kan därmed enligt vår mening inte anses omfatta behandling för arkivändamål. Mot den bakgrunden väcker enligt vår mening det faktum att regleringen i dataskyddsförordningen av rätten att behandla personuppgifter för arkivändamål framgår i anslutning till finalitetsprincipen (se avsnitt 8.4 frågor kring om man då kan tillämpa den del av bestämmelsen som tillåter arkivering.

I skäl 50 till dataskyddsförordningen anges att om behandling av personuppgifter 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

---

<sup>7</sup> Se Dataskyddsutredningens betänkande (SOU 2017:39).

<sup>8</sup> A.a. s. 216.

för vilka uppgifter och syften ytterligare behandling bör betraktas som förenlig och laglig. Därefter anges att ytterligare behandling för bl.a. arkivändamål av allmänt intresse bör betraktas som förenlig och laglig behandling av uppgifter. Detta skulle enligt vår mening kunna tolkas som att arkivering av personuppgifter alltid är tillåten, även om en registerförfattning har uttömmande ändamålsbestämmelser.

För att undanröja de tvivel som kan uppstå gällande detta och göra det helt klart för tillämparen att bestämmelserna i utlänningsdatalagen inte hindrar att personuppgifter behandlas för arkivändamål av allmänt intresse, anser vi att detta uttryckligen bör framgå av utlänningsdatalagen. Detta utgör enligt vår mening ett sådant införlivande av dataskyddsförordningen som är tillåtet enligt skäl 8 till förordningen (se avsnitt 5.3).

För att utlänningsdatalagens bestämmelse ska motsvara artikel 5.1 b i dataskyddsförordningen bör den utöver arkivändamål av allmänt intresse även omfatta vetenskapliga eller historiska forskningsändamål samt statistiska ändamål. Den bör även innehålla en hänvisning till artikel 89.1 i förordningen. På detta sätt klargörs att det även krävs sådana säkerhetsåtgärder som framgår av den senare bestämmelsen för att behandling för bl.a. arkivändamål ska vara tillåten. Vi behandlar dessa säkerhetsåtgärder i kommande avsnitt.

## **Personuppgifter som behandlats med stöd av brottsdatalagen**

Utredningen om 2016 års dataskyddsdirektiv har i sitt delbetänkande (SOU 2017:29 s.287) gjort bedömningen att behandling för arkivändamål omfattas av dataskyddsförordningens tillämpningsområde, oavsett om det är en i dataskyddsdirektivets mening behörig myndighet som arkiverar personuppgifterna eller om de överlämnas till en arkivmyndighet. För att ge ett konkret exempel; när Polismyndigheten utför gränskontroll i brottsbekämpande syfte kommer de aktuella personuppgifterna att behandlas enligt brottsdatalagen och Polismyndighetens registerförfattning. När handlingarna i ärendet därefter arkiveras kommer personuppgiftsbehandlingen däremot att utföras med stöd av dataskyddsförordningen

Enligt vad vi erfarit vid samråd med Utredningen om 2016 års dataskyddsdirektiv kommer den utredningen att ge förslag på en reglering av vilken prövning som ska göras innan personuppgifter, som behandlas med stöd av brottsdatalagen, får behandlas för ändamål utanför den lagens tillämpningsområde. Vi kommer därmed inte att behandla den frågan i vår promemoria.

## Hänvisning till dataskyddslagen och säkerhetsåtgärder

Som vi konstaterat i avsnitt 17.1.2 krävs det stöd i EU-rätten eller i nationell rätt för att känsliga personuppgifter ska få behandlas för arkivändamål av allmänt intresse (jfr artikel 9.2 j i dataskyddsförordningen).

Rätten att behandla personuppgifter (även känsliga) för arkivändamål framgår för närvarande genom utlänningsdatalagens hänvisning till 8 och 9 §§ PuL. Utlänningsdatalagens bestämmelser om under vilka förutsättningar känsliga personuppgifter får behandlas i övrigt är uttömmande (se kapitel 12). Mot den bakgrunden och då personuppgiftslagen ska upphävas, föreslår vi att stöd för att behandla känsliga personuppgifter även för arkivändamål skapas på utlänningsdatalagens tillämpningsområde genom en hänvisning till den föreslagna 3 kap. 6 § första stycket dataskyddslagen. Enligt denna bestämmelse får känsliga personuppgifter behandlas för arkivändamål av allmänt intresse om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om bevarande och vård av arkiv. Enligt Dataskyddsutredningens bedömning får arkivmaterial med stöd av 3 kap. 6 § dataskyddslagen även tas om hand av en arkivmyndighet.<sup>9</sup>

Vad gäller de skyddsåtgärder som enligt artikel 5.1 b, 9.2 j och 89.1 i dataskyddsförordningen krävs för de personuppgifter som behandlas för bl.a. arkivändamål av allmänt intresse kan följande sägas.

Skydd för arkiverade personuppgifter finns i svensk rätt i form av sekretessbestämmelser och gallringsföreskrifter. Vidare utgör de behörighets- och sökbegränsningar som finns i utlänningsdatalagen

---

<sup>9</sup> Se Dataskyddsutredningens betänkande (SOU 2017:39 s. 222).

sådana skyddsåtgärder som avses i dataskyddsförordningen. Ytterligare skyddsåtgärder för personuppgifter som behandlas för arkivändamål m.m. utgörs av utlänningsdatalagens bestämmelse om avskiljande och gallring. Våra överväganden i denna del finns i avsnitt 17.2.2 och 17.3.3.

Sammantaget anser vi att den befintliga regleringen i utlänningsdatalagen, tillsammans med övriga nationella föreskrifter, är tillräcklig för att säkerställa den registrerades rättigheter och intressen vid de aktuella myndigheternas behandling av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål.

För närvarande gäller 8 § andra stycket andra meningen och 9 § fjärde stycket PuL för personuppgiftsbehandling som utförs inom utlänningsdatalagens tillämpningsområde. Motsvarande bestämmelse kommer enligt Dataskyddsutredningens förslag att finnas i 4 kap. 1 § dataskyddslagen. Bestämmelsen innebär att personuppgifter som behandlas endast för arkivändamål av allmänt intresse inte får användas för att vidta åtgärder i fråga om den registrerade, om det inte finns synnerliga skäl för detta med hänsyn till den registrerades vitala intressen. Undantag görs dock för myndigheter som använder personuppgifter som finns i allmänna handlingar.

Vi föreslår att det i utlänningsdatalagen görs en hänvisning till 4 kap. 1 § dataskyddslagen. Genom en sådan hänvisning kommer det även fortsättningsvis att stå klart för tillämparen att de aktuella myndigheterna får återanvända de personuppgifter som finns i arkiverade ärenden. En förutsättning för detta är enligt vår mening dock att myndigheterna använder personuppgifterna för ett ändamål som omfattas av utlänningsdatalagen.

## **17.2 Avskiljande av personuppgifter**

### **17.2.1 Utlänningsdatalagen och utlänningsdataförordningen**

Av 22 § första stycket utlänningsdatalagen framgår att personuppgifter som har behandlats för ändamål som anges i 11 § 1–4 och 13 § i den lagen ska avskiljas så att tillgången till dem begränsas om de inte längre behövs i myndighetens löpande verksamhet. De personuppgifter som avses är de som har behandlats för hand-

läggning av ärenden eller för en myndighets biträde i ärenden, för kontroll av utlänningskontroll, för utförande av arbetsuppgifter som gäller mottagande och bosättning och för framställning av statistik. Även personuppgifter som har behandlats för att tillhandahålla information till andra myndigheter m.fl. avses.

Enligt 22 § andra stycket utlänningsdatalagen kan regeringen eller den myndighet som regeringen bestämmer, med stöd av 8 kap. 7 § regeringsformen, meddela ytterligare föreskrifter om avskiljande av personuppgifter. Genom 16 § utlänningsdataförordningen har regeringen gett Migrationsverket möjlighet att under vissa förutsättningar meddela föreskrifter om avskiljande av personuppgifter som behandlas av utlandsmyndigheterna under Migrationsverkets personuppgiftsansvar.

Av förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 103) framgår sammanfattningsvis följande. Arkivlagens bestämmelser om bevarande och gallring ska gälla för personuppgifter som behandlas automatiserat. Detta innebär ett behov av att överväga särskilda regler, som säkerställer att uppgifter som inte längre behövs i verksamheten bevaras i myndigheternas datasystem på ett sätt som gör att de inte finns tillgängliga för samtliga handläggare. Uppgifter som behandlas för ändamålen att handlägga ärenden, bedriva utlänningskontroll och mottagningsverksamhet är ofta av integritetskänslig karaktär och ofta tillgängliga för många anställda på myndigheterna. Regeringen anser därför att de uppgifter som inte längre är nödvändiga för den löpande verksamheten, t.ex. för att handläggningen av ett ärende har avslutats, ska avskiljas och inte längre vara tillgängliga för all den personal som arbetar i sådan verksamhet. Av 2014 års utlänningsdatautrednings betänkande (SOU 2015:76 s. 327) framgår att avskiljandet inte får innebära informationsförlust av något slag.

### 17.2.2 Bedömning

**Bedömning:** Dataskyddsförordningen föranleder ingen ändring av utlänningsdatalagens och utlänningsdataförordningens bestämmelser om avskiljande av personuppgifter.

Den personuppgiftsansvarige är, enligt artikel 24.1 och artikel 32 i dataskyddsförordningen, skyldig att se till att en lämplig säkerhetsnivå för behandlingen av personuppgifter upprätthålls. Detta ska, enligt samma bestämmelser, ske bl.a. genom att den personuppgiftsansvarige vidtar lämpliga tekniska och organisatoriska åtgärder. Den personuppgiftsansvariges skyldigheter i denna del återfinns även i de allmänna principer för behandling av personuppgifter som framgår av artikel 5.1 f i dataskyddsförordningen.

Utifrån den beskrivning av begreppet avskiljande som finns i förarbetena till utlänningsdatalagen (se föregående avsnitt) bör ett avskiljande innefatta en teknisk åtgärd som får till följd att de aktuella personuppgifterna inte längre är åtkomliga för all den personal som tidigare haft åtkomst till dem. Beroende på vilka andra säkerhetsåtgärder som vidtas (t.ex. om loggning sker och vilken uppföljning av loggningen som i så fall utförs) torde avskiljandet innebära att den personuppgiftsansvariga myndigheten får bättre kontroll över vilka anställda som bereder sig tillgång till de aktuella uppgifterna.

Huvudregeln för behandling av personuppgifter är, både enligt personuppgiftslagen och enligt dataskyddsförordningen, att uppgifterna inte får bevaras/förvaras under längre tid än vad som är nödvändigt för de ändamål för vilka de behandlas (se 9 § första stycket i PuL och artikel 5.1 e i dataskyddsförordningen). Undantag görs dock för personuppgifter som behandlas för arkivändamål (9 § tredje stycket PuL och artikel 5.1 e i dataskyddsförordningen). Ett exempel på personuppgifter som ska avskiljas är uppgifter som finns i handlingar som tagits om hand för arkivering av myndigheten.<sup>10</sup>

Åtgärder som säkerställer en lämplig säkerhetsnivå ska förvisso vidtas av de personuppgiftsansvariga även utan bestämmelser i registerförfattningar. Vi anser dock att bestämmelser om vilka säkerhetsåtgärder som ska vidtas i en viss verksamhet utgör sådana specifika krav på personuppgiftsbehandling som enligt artikel 6.2 i dataskyddsförordningen får fastställas genom nationella registerförfattningar (se kapitel 5). Dataskyddsförordningen hindrar därmed inte att utlänningsdatalagens materiella bestämmelser om avskiljande finns kvar.

---

<sup>10</sup> Se 2014 års utlänningsdatautrednings betänkande (SOU 2015:73 s. 327 f.).

I sitt betänkande (SOU 2015:73 s. 327 f.) har 2014 års utlänningsdatautredning gjort noggranna överväganden av behovet att avskilja personuppgifter inom utlänningsdatalagens tillämpningsområde och av vilka personuppgifter som ska omfattas av denna skyldighet. Dessa överväganden har legat till grund för den reglering som finns i dag. I avsnitt 18.2 gör vi vidare bedömningen att dataskyddsförordningen inte hindrar att nationella bestämmelser om personuppgiftsbehandling införs i en förordning eller i en myndighetsföreskrift, så länge föreskrifterna tillkommit i laga ordning.

Mot den bakgrunden och med hänsyn till ramen för vårt uppdrag, anser vi att utlänningsdatalagens och utlänningsdataförordningens bestämmelser om avskiljande av personuppgifter samt om föreskriftsrätten på området ska finnas kvar i sin nuvarande lydelse.

## **17.3 Gallring av personuppgifter**

### **17.3.1 Arkivreglerna i korthet**

Av 10 § arkivlagen (1990:782) framgår att allmänna handlingar får gallras, men att det vid gallring alltid ska beaktas bl.a. att arkiven utgör en del av kulturarvet och att det arkivmaterial som återstår ska kunna tillgodose syftet med arkivbildningen. Detta syfte framgår av 3 § tredje stycket arkivlagen och utgörs av rätten att ta del av allmänna handlingar, behovet av information för rättskipningen och förvaltningen samt forskningens behov. Av 10 § tredje stycket arkivlagen framgår att avvikande bestämmelser om gallring i annan lag eller i förordning gäller i stället för arkivlagens bestämmelser. Enligt 14 § arkivförordningen (1991:446) får statliga myndigheter gallra allmänna handlingar endast i enlighet med föreskrifter eller beslut av Riksarkivet, om inte särskilda gallringsföreskrifter finns i lag eller förordning.

### **17.3.2 Utlänningsdatalagen och utlänningsdataförordningen**

Många svenska registerförfattningar, däribland utlänningsdatalagen, innehåller bestämmelser om gallring. Enligt 15 § andra

stycket 2 utlänningsdatalagen har regeringen rätt att meddela föreskrifter om gallring av känsliga personuppgifter. Några sådana föreskrifter finns dock inte i utlänningsdataförordningen. Regeringen har även, enligt 14 § tredje stycket 2 utlänningsdatalagen, rätt att meddela föreskrifter om gallring vad gäller Migrationsverkets register över fingeravtryck och fotografier. Denna rätt har regeringen utnyttjat genom att i 3 § utlänningsdataförordningen föreskriva att en uppgift i detta register ska gallras när den registrerade blir svensk medborgare och i andra fall senast tio år efter det att uppgiften registrerades. Som vi nämnt i föregående avsnitt har de gallringsbestämmelser som finns i utlänningsdatalagen eller i föreskrifter som har meddelats i anslutning till den lagen, företräde före den rätt att arkivera och bevara handlingar som framgår av 8 § andra stycket PuL (8 § andra stycket utlänningsdatalagen).

I förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 77 och 102) gjorde regeringen följande bedömning. Dagens teknik medför att en i princip obegränsad mängd personuppgifter kan bevaras elektroniskt hos myndigheterna. Ett elektroniskt bevarande ökar möjligheten att på ett enkelt sätt söka och sammanställa uppgifter, något som också kan öka risken för integritetsintrång. En metod att minska integritetskänsligheten är att se till att uppgifter som inte längre behövs i en myndighets verksamhet gallras ur myndighetens datasystem. Det finns omständigheter som talar för att särskilda bestämmelser om gallring ska införas i utlänningsdatalagen, bl.a. mängden personuppgifter och registrerade samt att behandlingen i många fall sker i myndighetsutövning och utan den enskildes samtycke. Många av personuppgifterna är dessutom integritetskänsliga. De omständigheter som talar mot särskilda gallringsbestämmelser är bl.a. att utgångspunkten är att automatiserat behandlade personuppgifter i allmänna handlingar ska bevaras. Det finns också ofta ett behov av att ta fram uppgifter från tidigare ärenden vid handläggning av ärenden hos Migrationsverket. Vidare talar allmänhetens intresse av insyn i verksamheten för att bevarande bör vara utgångspunkten. Mot denna bakgrund bedömer regeringen att någon generell gallringsbestämmelse inte bör föras in i utlänningsdatalagen. Det kan dock finnas behov av vissa specifika gallringsregler, särskilt när det gäller känsliga personuppgifter. Dessa behöver kunna utformas



på ett sätt som är anpassat till den tekniska utvecklingen och Migrationsverkets över tid varierande behov. Det är därför mest lämpligt att gallringsbestämmelser ges på förordningsnivå.

### 17.3.3 Bedömning

**Bedömning:** Dataskyddsförordningen föranleder inte någon ändring i sak av utlänningsdatalagens och utlänningsdataförordningens bestämmelser om gallring.

Av förarbetena till utlänningsdatalagen framgår att avsikten med de befintliga gallringsbestämmelserna har varit att främja de registrerades personliga integritet. Det faktum att arkivlagstiftningens gallringsbegrepp används och att åtgärden därmed innebär att de aktuella uppgifterna raderas även om de finns i allmänna handlingar får också till följd att bestämmelserna fullt ut får den avsedda effekten (jfr 10 § tredje stycket arkivlagen och 14 § arkivförordningen).

Utredningen om 2016 års dataskyddsdirektiv har i sitt delbetänkande (SOU 2017:29 s. 282 ff.) föreslagit att – vid implementeringen av direktivet – orden bevarande och gallring bara ska användas i den betydelse de har i arkivlagstiftningen. Syftet med detta uppges vara att tydligare skilja mellan arkivrättsliga regler och regler om dataskydd. Utredningen anför att gallringsbestämmelserna i myndigheternas registerförfattningar syftar till att skydda de enskildas integritet, medan gallring enligt Riksarkivets föreskrifter görs för att begränsa arkivens omfattning. I brottsdatalagen och dess tillhörande registerförfattningar bör, enligt utredningen, regleringen därför i stället utgå från hur länge personuppgifter får behandlas för andra ändamål än arkivändamål. Det är rimligt att anta att förslaget innebär att bestämmelser om gallring kommer att utmönstras ur dessa registerförfattningar och ersättas med en sådan reglering. Utredningen kommer dock inte förrän i sitt slutbetänkande att ge förslag till hur de registerförfattningar som kompletterar brottsdatalagen ska förändras.

Som vi redogjort för i avsnitt 17.2.2 innebär ett avskiljande av personuppgifter att endast en begränsad krets anställda har teknisk åtkomst till dem. Gallring innebär i sin tur att personuppgifterna

raderas eller åtminstone att information går förlorad, även om uppgifterna finns i sådana allmänna handlingar som enligt huvudregeln ska tas om hand för arkivering. Den typ av begränsning av behandling som Utredningen om 2016 års dataskyddsdirektiv beskriver i sitt delbetänkande skulle, som vi förstår det, innebära att de aktuella uppgifterna finns kvar i myndigheternas databaser om de ingår i sådana allmänna handlingar som ska arkiveras. En sådan bestämmelse skulle därmed inte innebära samma definitiva förlust av information som en gallringsbestämmelse, men ändå utgöra ett skydd för de registrerades personliga integritet. Detta förefaller enligt vår mening vara en ändamålsenlig reglering.

Utredningen om 2016 års dataskyddsdirektivs förslag har emellertid ännu inte lett till lagstiftning. Eftersom gallringsbestämmelserna utgör ett skydd för de registrerades integritet (jfr artikel 5.1 f, artikel 24.1 och artikel 32 i dataskyddsförordningen) föranleder dataskyddsförordningen enligt vår bedömning inte heller någon ändring av bestämmelserna. Dessa är snarare i linje med dataskyddsförordningens huvudregel att personuppgifter inte ska behandlas (dvs. inte ens lagras) längre än vad som behövs för de ändamål som uppgifterna behandlas för. I avsnitt 18.2 gör vi vidare bedömningen att dataskyddsförordningen inte hindrar att nationella bestämmelser om personuppgiftsbehandling införs i en förordning eller i en myndighetsföreskrift, så länge föreskrifterna tillkommit i laga ordning. Mot den bakgrunden bedömer vi att utlänningsdatalagens och utlänningsdataförordningens materiella bestämmelser om gallring samt om regeringens föreskriftsrätt på området kan finnas kvar oförändrade.

När dataskyddsförordningen börjar tillämpas ska personuppgiftslagen upphävas.<sup>11</sup> Det krävs därmed redaktionella ändringar i den bestämmelse som reglerar förhållandet mellan utlänningsdatalagens bestämmelser om gallring och rätten att behandla uppgifter för arkivändamål (för närvarande en hänvisning till personuppgiftslagen i 8 § andra stycket utlänningsdatalagen). Man kan förvisso, enligt vår bedömning, diskutera om bestämmelsen egentligen tillför något. Gallringsbestämmelser i annan lag eller förordning har företräde före arkivlagens bestämmelser (10 § tredje stycket arkivlagen). Personuppgifter som har gallrats med stöd av utlännings-

---

<sup>11</sup> Se kommittédirektiv till Dataskyddsutredningen (Dir 2016:15 s. 6).

datalagen kan rimligtvis inte arkiveras. Bestämmelsen har vid utlänningsdatalagens tillkomst dock ansetts fylla en klargörande funktion.<sup>12</sup> Mot den bakgrunden och med hänsyn till att dataskyddsförordningen inte föranleder någon ändring av bestämmelsen, anser vi att den kan finnas kvar. Den bör dock placeras i anslutning till den bestämmelse om rätten att behandla bl.a. personuppgifter för arkivändamål som vi har föreslagit (avsnitt 17.1.4).

---

<sup>12</sup> Se förarbetena till utlänningsdatalagen (prop. 2015/16:65 s. 48).



## 18 Föreskriftsrätten

### 18.1 Utlänningsdatalagen och utlänningsdataförordningen

Utlänningsdatalagen och utlänningsdataförordningen innehåller en mängd bestämmelser om föreskriftsrätt för regeringen eller de myndigheter regeringen bestämmer (i praktiken Migrationsverket och Polismyndigheten). Exempelvis får regeringen eller den myndighet som regeringen bestämmer, enligt 23 § utlänningsdatalagen, meddela föreskrifter om säkerhetsåtgärder till skydd för personuppgifter. Regeringen har utnyttjat denna föreskriftsrätt genom att, i 17 § utlänningsdataförordningen, ge Migrationsverket rätt att under vissa förutsättningar meddela föreskrifter om säkerhetsåtgärder till skydd för personuppgifter som behandlas av utlandsmyndigheterna under Migrationsverkets personuppgiftsansvar. Enligt 18 och 19 §§ utlänningsdataförordningen får Migrationsverket respektive Polismyndigheten vidare meddela ytterligare föreskrifter om verkställighet av utlänningsdatalagen och utlänningsdataförordningen inom sina ansvarsområden. Av 20 § utlänningsdataförordningen framgår att Migrationsverket och Polismyndigheten ska ge Datainspektionen tillfälle att yttra sig innan de meddelar föreskrifter med stöd av förordningen i frågor som berör särskilda risker för intrång i den personliga integriteten. I övrigt behandlar vi utlänningsdatalagens och utlänningsdataförordningens bestämmelser om föreskriftsrätt i tidigare kapitel (se bl.a. kapitel 12, 13 och 17).

## 18.2 Bedömning

**Bedömning:** Dataskyddsförordningen föranleder ingen ändring av utlänningsdatalagens och utlänningsdataförordningens bestämmelser om föreskriftsrätt.

Medlemsstaterna har, enligt artikel 6.2 och 6.3 i dataskyddsförordningen, rätt att i nationell lagstiftning behålla eller införa mer specifika bestämmelser för personuppgiftsbehandling. Detta kan ske exempelvis genom nationella registerförfattningar (se vidare kapitel 5). Varken artikel 6.2 eller 6.3 innehåller något krav på att de bestämmelser som avses måste regleras i lag. Det är därmed vår uppfattning att det bör vara upp till den enskilda medlemsstaten på vilken nivå i normhierarkin sådana bestämmelser införs. I enlighet med detta ställningstagande hindrar dataskyddsförordningen inte att bestämmelser om personuppgiftsbehandling införs i en förordning eller i en myndighetsföreskrift. Detta förutsätter naturligtvis att föreskrifterna tillkommit i laga ordning.

Mot den bakgrunden anser vi att dataskyddsförordningen inte föranleder någon ändring av den föreskriftsrätt som genom utlänningsdatalagens och utlänningsdataförordningens bestämmelser tilldelats regeringen, Migrationsverket och Polismyndigheten.

# 19 Överklagandebestämmelser

## 19.1 Utlänningsdatalagen och personuppgiftslagen

Utlänningsdatalagen hänvisar, genom 8 § första stycket 13, till 51 § första stycket, 52 § första stycket och 53 § PuL.

Enligt 51 § första stycket PuL får tillsynsmyndighetens beslut enligt personuppgiftslagen om annat än föreskrifter överklagas hos allmän förvaltningsdomstol.

Av 52 § första stycket PuL framgår att en myndighets beslut enligt den lagen i vissa fall får överklagas hos allmän förvaltningsdomstol. Detta gäller beslut om information enligt 26 §, om rättelse och underrättelse till tredje man enligt 28 §, om information enligt 29 § andra stycket och om upplysningar enligt 42 §. Av förarbetena till 52 § PuL (prop. 2005/06:173 s. 51 f.) framgår att möjligheten att överklaga de beslut som myndigheter fattar i sin egenskap av personuppgiftsansvariga inte har sin grund i 1995 års dataskyddsdirektiv, utan motiveras av allmänna förvaltningsrättsliga principer om att förvaltningsbeslut som direkt berör en enskild person ska kunna överprövas av domstol.

Enligt 53 § PuL får andra beslut enligt den lagen än de som avses i 47, 51 och 52 §§ inte överklagas. Indirekt regleras här således en överklaganderätt vad gäller de beslut som en förvaltningsrätt enligt 47 § PuL har fattat efter en ansökan av tillsynsmyndigheten om att personuppgifter som har behandlats på ett olagligt sätt ska utplånas.

## 19.2 Dataskyddsförordningen och stadgan

Artikel 78 i dataskyddsförordningen reglerar rätten till ett effektivt rättsmedel mot tillsynsmyndighetens beslut. Här framgår att varje fysisk eller juridisk person har rätt till ett effektivt rättsmedel mot

ett rättsligt bindande beslut som meddelats av en tillsynsmyndighet rörande dem (led 1). Det framgår också att varje registrerad person har rätt till ett effektivt rättsmedel om den behöriga tillsynsmyndigheten inte behandlar ett klagomål. Detsamma gäller om tillsynsmyndigheten inte informerar den registrerade inom tre månader om hur arbetet med det klagomål som getts in fortskrider eller vilket beslut som har fattats med anledning av klagomålet (led 2). Att det är ett domstolsförfarande som avses i led 1 och 2 förstås av led 3. Här framgår att talan mot en tillsynsmyndighet ska väckas vid domstolarna i den medlemsstat där tillsynsmyndigheten har sitt säte.

Enligt artikel 79.1 i dataskyddsförordningen har alla registrerade rätt till ett effektivt rättsmedel om de anser att deras rättigheter enligt förordningen har åsidosatts som en följd av att deras personuppgifter har behandlats på ett sätt som inte är förenligt med förordningen. Enligt bestämmelsen gäller detta utöver rätten att lämna in ett klagomål till tillsynsmyndigheten. Om den personuppgiftsansvarige eller personuppgiftsbiträdet är en myndighet som agerar inom ramen för sin myndighetsutövning ska sådan talan, enligt artikel 79.2 i dataskyddsförordningen, väckas vid domstolarna i den medlemsstat där den personuppgiftsansvarige – eller personuppgiftsbiträdet – är etablerad.

Den registrerade har vidare, enligt artikel 82 i dataskyddsförordningen, rätt till skadestånd vid överträdelser av förordningens bestämmelser.

Rätten till ett effektivt rättsmedel garanteras även av Europeiska unionens stadga om de grundläggande rättigheterna. Denna rätt, som kommer till uttryck i artikel 47 i stadgan, omfattar de rättigheter som garanteras av unionsrätten. Vad gäller personuppgiftsbehandling ger artikel 8.1 i stadgan var och en rätt till skydd av sådana uppgifter som rör honom eller henne. Som en konkretisering av denna rättighet anges i artikel 8.2 att personuppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av en legitim och lagenlig grund. Var och en har dessutom rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dessa uppgifter. Enligt artikel 8.3 ska en oberoende myndighet kontrollera att dessa regler efterlevs.



## 19.3 Dataskyddslagen

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) föreslagit att 8 kap. dataskyddslagen ska innehålla bestämmelser om skadestånd och andra rättsmedel. Rätten till skadestånd behandlas i avsnitt 14.8 i vår promemoria. Vad gäller övriga rättsmedel innehåller förslaget till dataskyddslag följande reglering.

### 19.3.1 Överklagande av en myndighets beslut

Enligt den föreslagna 8 kap. 2 § dataskyddslagen får beslut enligt artiklarna 12.5, 15–19 eller 21 i dataskyddsförordningen som har meddelats av en myndighet i egenskap av personuppgiftsansvarig överklagas till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten och rätten att överklaga gäller inte beslut som fattats av riksdagen, regeringen, Högsta domstolen, Högsta förvaltningsdomstolen eller riksdagens ombudsmän.

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39 s. 303) sammanfattningsvis gjort följande bedömning.

De förvaltningsrättsliga principer som motiverar att denna typ av beslut ska kunna överprövas av domstol gör sig gällande även avseende vissa av de beslut som personuppgiftsansvariga myndigheter kommer att fatta enligt dataskyddsförordningen till följd av en registrerads begäran. Även dataskyddslagen bör därför förse med en uttrycklig bestämmelse om att vissa myndighetsbeslut får överklagas till allmän förvaltningsdomstol. Rätten att överklaga bör omfatta beslut som en personuppgiftsansvarig myndighet fattar med anledning av att en registrerad utövar sina rättigheter enligt tredje kapitlet 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).

### 19.3.2 Dröjsmålstalan

Dataskyddsförordningen garanterar – genom artikel 78.2 – att en registrerad som med stöd av förordningen har lämnat in ett klagomål till tillsynsmyndigheten har rätt till ett effektivt rättsmedel, om myndigheten inte handlägger klagomålet eller tar lång tid på sig. För att uppfylla detta krav finns i den föreslagna 6 kap. 5 § dataskyddslagen bestämmelser om den registrerades rätt att under vissa förutsättningar få besked av tillsynsmyndigheten angående handläggningen av ett klagomål. Enligt vårt förslag ska bestämmelsen i 6 kap. 5 § dataskyddslagen gälla även på utlänningsdatalagens tillämpningsområde (se avsnitt 9.4.10).

Enligt förslaget till 8 kap. 3 § dataskyddslagen får tillsynsmyndighetens beslut att avslå en begäran om besked enligt 6 kap. 5 § samma lag 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.

Dataskyddsutredningen anför i sitt betänkande (SOU 2017:39 s. 328 f.) sammanfattningsvis följande.

Skyndsamhetskrav och informationsskyldighet gäller redan enligt förvaltningslagens allmänna bestämmelser och eventuella brister i handläggningen kan anmälas till och bli föremål för prövning av riksdagens ombudsmän (JO). 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.

### 19.3.3 Överklagande av tillsynsmyndighetens beslut

Enligt den föreslagna 8 kap. 4 § dataskyddslagen får tillsynsmyndighetens beslut enligt dataskyddsförordningen och enligt 7 kap. 1 och 2 §§ dataskyddslagen överklagas till allmän förvaltningsdomstol. Vid överklagande till kammarrätten krävs prövningstillstånd.

De föreslagna 7 kap. 1 och 2 §§ dataskyddslagen avser beslut om administrativa sanktionsavgifter. Enligt vårt förslag ska dataskyddslagens bestämmelse i 7 kap. 1 §, men inte i 7 kap. 2 §, gälla på utlänningsdatalagens tillämpningsområde (se avsnitt 9.4.14).

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39 s. 325 ff.) sammanfattningsvis gjort följande ställningstagande.

Den rätt till ett effektivt rättsmedel mot tillsynsmyndighetens beslut som framgår av artikel 78.1 i dataskyddsförordningen tillgodoses i svensk rätt normalt genom möjligheten att överklaga beslutet till allmän förvaltningsdomstol. Rätten att överklaga bör uttryckligen anges i dataskyddslagen och 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. Formerna för överklagande av tillsynsmyndighetens beslut, vilken överklagandefrist som ska gälla, talerätt m.m., bör inte avvika från förvaltningslagens bestämmelser.

### 19.3.4 Beslut om enskilt organs behandling för arkivändamål

Av den föreslagna 8 kap. 5 § dataskyddslagen framgår att beslut enligt 2 kap. 5 § andra stycket, 3 kap. 6 § tredje stycket och 3 kap. 10 § den lagen får överklagas till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten.

I 2 kap. 5 § andra stycket dataskyddslagen behandlas rätten för myndighet (Riksarkivet) att i enskilda fall besluta att enskilda organ får behandla personuppgifter för arkivändamål av allmänt intresse. Enligt 3 kap. 6 § tredje stycket dataskyddslagen får

myndighet (Riksarkivet) på motsvarande sätt fatta beslut som tillåter enskilda organ att behandla känsliga personuppgifter för sådana ändamål. Bestämmelserna är enligt vår bedömning inte relevanta inom utlänningsdatalagens tillämpningsområde.

Bestämmelsen i 3 kap. 10 § dataskyddslagen gäller myndighets beslut att i enskilda fall tillåta behandling av personuppgifter som rör fällande domar i brottmål, lagöverträdelse som innefattar brott eller straffprocessuella tvångsmedel. Myndigheter får dock, enligt artikel 10 i dataskyddsförordningen, behandla sådana uppgifter även utan beslut av tillsynsmyndigheten. Därmed är inte heller 3 kap. 10 § dataskyddslagen relevant inom utlänningsdatalagens tillämpningsområde.

### 19.3.5 Uttömmande överklagandebestämmelser

Av den föreslagna 8 kap. 6 § dataskyddslagen framgår att andra beslut enligt lagen än de som avses i 8 kap. 2–5 §§ och 6 kap. 2 § inte får överklagas.

## 19.4 Bedömning

**Förslag:** Beslut som Migrationsverket, utlandsmyndigheterna och Polismyndigheten meddelat i egenskap av personuppgiftsansvariga inom utlänningsdatalagens tillämpningsområde enligt artiklarna 12.5, 15–19 eller 21 i dataskyddsförordningen ska få överklagas till allmän förvaltningsdomstol. Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Tillsynsmyndighetens beslut att avslå en begäran om besked enligt den föreslagna 6 kap. 5 § dataskyddslagen ska få 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 ska inte få överklagas.

Tillsynsmyndighetens beslut enligt dataskyddsförordningen och enligt den föreslagna 7 kap. 1 § dataskyddslagen ska få

överklagas till allmän förvaltningsdomstol. Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Andra beslut ska inte få överklagas.

Bestämmelserna ska genomföras genom hänvisningar i utlänningsdatalagen till de föreslagna 8 kap. 2–4 samt 6 §§ dataskyddslagen.

Dataskyddsutredningen har gjort bedömningen att de beslut som en personuppgiftsansvarig myndighet fattar med anledning av att en registrerad utövar sina rättigheter enligt tredje kapitlet i dataskyddsförordningen bör gå att överklaga. Vi finner inte anledning att göra någon annan bedömning för de beslut som fattas av myndigheterna inom utlänningsdatalagens tillämpningsområde i deras egenskap av personuppgiftsansvariga myndigheter. Ställningstagandet stämmer vidare överens med vad som för närvarande gäller; genom utlänningsdatalagens hänvisning till 52 § PuL får bl.a. sådana beslut som gäller information till den registrerade, rättelse och underrättelse till tredje man överklagas. Mot den bakgrunden föreslår vi att det tas in en hänvisning i utlänningsdatalagen till 8 kap. 2 § dataskyddslagen.

Vi har föreslagit att den registrerades rätt att enligt 6 kap. 5 § dataskyddslagen få besked om handläggningen av ett klagomål ska vara tillämplig även på utlänningsdatalagens tillämpningsområde (se avsnitt 9.4.10). Mot den bakgrunden anser vi att det i utlänningsdatalagen även bör göras en hänvisning till 8 kap. 3 § dataskyddslagen, som reglerar överklagande av sådana beslut. Den nya förvaltningslagen, som kommer att träda i kraft den 1 juli 2018, kommer i och för sig att innehålla en liknande generell bestämmelse om dröjsmålstalan.<sup>1</sup> Med hänsyn till att det är angeläget att systematiken i utlänningsdatalagen - i den mån det är möjligt - följer dataskyddslagen anser vi trots detta att möjligheten att väcka dröjsmålstalan bör regleras i utlänningsdatalagen.

Regleringen i 8 kap. 4 § dataskyddslagen är en följd av dataskyddsförordningens bestämmelser om rätten till ett effektivt rättsmedel mot tillsynsmyndighetens beslut. Denna rätt gör sig enligt vår mening gällande även för de myndigheter som hanterar

---

<sup>1</sup> Se riksdagsskrivelse 2017/18:2.

personuppgifter inom ramen för utlännings- och medborgarskapslagstiftningen. För dessa myndigheter är de delar av 8 kap. 4 § dataskyddslagen som rör överklagande av beslut enligt 7 kap. 2 § dataskyddslagen visserligen inte relevanta (se avsnitt 19.3.3). Anledningen till detta är helt enkelt att tillsynsmyndigheten inte bör komma att fatta några beslut enligt denna bestämmelse mot de aktuella myndigheterna, eftersom myndigheter har rätt att behandla personuppgifter som rör fällande domar i brottmål, lagöverträdelser som innefattar brott eller straffprocessuella tvångsmedel. En hänvisning till 8 kap. 4 § i sin helhet är emellertid en enklare lagteknisk lösning. En hänvisning även till de delar av bestämmelsen som inte är relevanta för de aktuella myndigheterna får inte heller någon betydelse. Vi anser därför att en hänvisning till 8 kap. 4 § dataskyddslagen i sin helhet bör göras i utlänningsdatalagen.

Sammanfattningsvis föreslår vi således att det i utlänningsdatalagen ska tas in hänvisningar till 8 kap. 2–4 §§ dataskyddslagen. Genom dessa hänvisningar kommer (i tillämpliga delar) de bestämmelser för överklagande som generellt gäller för myndigheter att gälla även för de myndigheter som behandlar personuppgifter inom utlänningsdatalagens tillämpningsområde. Vidare garanteras rätten till ett effektivt rättsmedel i artikel 78.1 i dataskyddsförordningen, eftersom både fysiska och juridiska personer ges rätt till domstolsprövning av de beslut som tillsynsmyndigheten har fattat rörande dem. Den registrerade ges också rätt till domstolsprövning vid ett sådant dröjsmål i tillsynsmyndighetens handläggning som omfattas av artikel 78.2 i dataskyddsförordningen.

De bestämmelser vi föreslagit medför vidare att den registrerade har rätt att överklaga de beslut som de aktuella myndigheterna fattar rörande honom eller henne i egenskap av personuppgiftsansvariga myndigheter, förutsatt att besluten rör den registrerades rättigheter enligt dataskyddsförordningen och stadgan. Vi föreslår dessutom att den registrerade ska ha rätt att begära skadestånd av den personuppgiftsansvariga myndigheten (se avsnitt 14.8). Vi anser att detta innebär att samtliga rättigheter till ett effektivt rättsmedel som föreskrivs i dataskyddsförordningen garanteras genom våra förslag. Vi bedömer också att de rättigheter som anges i artikel 8 i kombination med artikel 47 i stadgan garanteras av de

överklagandebestämmelser vi föreslagit (rätt till lagenlig behandling för bestämda ändamål, rätt till tillgång till och rättelse av de egna personuppgifterna samt rätt till ett effektivt rättsmedel inför en domstol om dessa rättigheter har kränkts).

Mot den bakgrunden anser vi att en hänvisning även bör göras till den föreslagna 8 kap. 6 § dataskyddslagen, som innebär att inga andra beslut än sådana som avses i 8 kap. 2–5 §§ dataskyddslagen samt sådana som avses i 6 kap. 2 § samma lag får överklagas. Enligt vårt förslag ska 6 kap. 2 § dataskyddslagen vara tillämplig på utlänningsdatalagens område (se avsnitt 9.4.10).





## 20 Övergångs- och ikraftträdandebestämmelser

### 20.1 Två olika ikraftträdandedatum

**Förslag:** Ändringen i bestämmelsen om utlänningsdatalagens förhållande till Polismyndighetens brottsbekämpande verksamhet och bestämmelsen om lagens förhållande till brottsdatalagen ska träda i kraft den 1 maj 2018.

Övriga ändringar i utlänningsdatalagen och utlänningsdataförordningen ska träda i kraft den 25 maj 2018.

Dataskyddsförordningen ska, enligt artikel 99.2 i förordningen, börja tillämpas den 25 maj 2018. Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) föreslagit att dataskyddslagen ska träda i kraft vid den tidpunkten. Eftersom utlänningsdatalagen kommer att utgöra en komplettering till dataskyddsförordningen och innehålla hänvisningar till dataskyddslagen bör även våra författningsförslag träda i kraft den 25 maj 2018.

Ikraftträdandebestämmelserna kompliceras dock något av att den tidpunkt då dataskyddsförordningen ska börja tillämpas och den tidpunkt då brottsdatalagen föreslås träda i kraft inte sammanfaller med varandra. Som en följd av bestämmelserna i 2016 års dataskyddsdirektiv har Utredningen om 2016 års dataskyddsdirektiv i sitt betänkande (SOU 2017:29) föreslagit att brottsdatalagen ska träda i kraft den 1 maj 2018. Enligt vårt förslag ska utlänningsdatalagen och utlänningsdataförordningen inte gälla vid behandling av personuppgifter i sådan verksamhet som omfattas av brottsdatalagens tillämpningsområde (se avsnitt 7.2.4). Detta tillämpningsområde är vidare än den avgränsning mot Polismyndighetens brottsbekämpande verksamhet som för närvarande

finns i 3 § utlänningsdatalagen. Följden av detta blir att om hela vårt författningsförslag skulle träda i kraft först den 25 maj 2018 skulle de delar av Polismyndighetens verksamhet som inte utgör brottsbekämpande verksamhet, men som ändå faller under brottsdatalagens tillämpningsområde dubbelregleras under perioden den 1–24 maj 2018. Som exempel kan nämnas Polismyndighetens verkställighet av beslut om utvisning på grund av brott enligt 8 a kap. utlänningslagen (2005:716). I 2014 års utlänningsdatautrednings betänkande (SOU 2015:73 s. 228 f.) görs bedömningen att sådan verksamhet faller under utlänningsdatalagens tillämpningsområde. Med hänsyn till att brottsdatalagen kommer att omfatta behandling av personuppgifter som görs i syfte att verkställa straffrättsliga påföljder är det enligt vår mening rimligt att anta att denna verksamhet kommer att omfattas av den lagen.<sup>1</sup>

Med särskilda ikraftträdandebestämmelser för den del av vårt förslag som reglerar förhållandet till brottsdatalagen kan en dubbelreglering emellertid undvikas. Vi föreslår därför att den nya lydelsen av 3 § utlänningsdatalagen och den av oss föreslagna 3 a §, vilka reglerar förhållandet till brottsbekämpande verksamhet respektive brottsdatalagen, ska träda i kraft redan den 1 maj 2018.

I övriga delar bör våra förslag träda i kraft den 25 maj 2018. Med anledning av att utlänningsdataförordningen innehåller kompletterande forskrifter om sådan behandling av personuppgifter som omfattas av utlänningsdatalagen får den särskilda ikraftträdandebestämmelsen för 3 och 3 a §§ utlänningsdatalagen genomslag även för förordningen.

## 20.2 Pågående ärenden

**Bedömning:** Den föreslagna övergångsbestämmelsen till dataskyddslagen som reglerar att äldre föreskrifter fortfarande gäller för ärenden hos Datainspektionen som har inletts men inte avgjorts före ikraftträdandet, gäller även på utlänningsdatalagens tillämpningsområde.

<sup>1</sup> Se Utredningen om 2016 års dataskyddsdirektivs delbetänkande (SOU 2019:29 s. 194 f. och 198 f.).

Datainspektionen har befogenhet att vidta åtgärder mot myndigheterna i deras egenskap av personuppgiftsansvariga. Datainspektionen kan exempelvis förbjuda den personuppgiftsansvarige att behandla personuppgifter på något annat sätt än att lagra dem eller ansöka om utplåning av personuppgifter hos allmän förvaltningsdomstol. Datainspektionen får vidare besluta om säkerhetsåtgärder som den personuppgiftsansvarige ska vidta. De materiella bestämmelserna finns i 32 §, 43 och 44 §§, 45 § första stycket och 47 § PuL, till vilka utlänningsdatalagen hänvisar genom 8 § första stycket 7 och 11.

Som framgår av avsnitt 20.1 har Dataskyddsutredningen föreslagit att dataskyddslagen ska träda i kraft den 25 maj 2018. Vid samma tidpunkt föreslår den utredningen att personuppgiftslagen ska upphävas. I Dataskyddsutredningens betänkande (SOU 2017:39) finns emellertid förslag på en övergångsbestämmelse som innebär att äldre föreskrifter fortfarande gäller för ärenden hos Datainspektionen som har inletts men inte avgjorts före ikraftträdandet. Som skäl för detta har utredningen anfört att exempelvis förelägganden om säkerhetsåtgärder eller radering inte kan baseras på dataskyddsförordningens bestämmelser innan dessa är tillämpliga. Med äldre föreskrifter menas enligt Dataskyddsutredningen personuppgiftslagen, personuppgiftsförordningen och föreskrifter som meddelats med stöd av dessa.<sup>2</sup>

Datainspektionens ärenden gentemot de myndigheter som är utpekade personuppgiftsansvariga enligt utlänningsdatalagen drivs enligt vår mening med stöd av personuppgiftslagens bestämmelser och handläggs enligt den lagens regelverk. En annan sak är att Datainspektionen i sin tillsyn inte bara bedömer om en personuppgiftsansvarig myndighet har behandlat personuppgifter i enlighet med personuppgiftslagen, utan även beaktar tillämplig registerförfattning, som t.ex. utlänningsdatalagen. Mot den bakgrunden bedömer vi att dataskyddslagens föreslagna övergångsbestämmelse är tillämplig även på de eventuella ärenden som Datainspektionen har inlett mot de myndigheter som omfattas av utlänningsdatalagen men som inte har avgjorts när våra författningsförslag träder i kraft. Någon särskild övergångs-

---

<sup>2</sup> Se Dataskyddsutredningens betänkande (SOU 2017:39 s. 340 ff.).

bestämmelse i utlänningsdatalagen som täcker sådana ärenden behövs enligt vår mening därmed inte.

### 20.3 Beslut som har meddelats före ikraftträdandet

**Förslag:** Äldre föreskrifter ska fortfarande gälla för överklagande av beslut som har meddelats med stöd av de föreskrifterna.

Bestämmelser om överklagande av vissa beslut som fattats med stöd av personuppgiftslagen finns i 51–53 §§ PuL. Av 51 och 52 §§ framgår att Datainspektionens beslut respektive beslut av en personuppgiftsansvarig myndighet i vissa fall får överklagas till allmän förvaltningsdomstol. Enligt 53 § får även en förvaltningsrätts beslut efter Datainspektionens ansökan om utplåning av personuppgifter överklagas. Utlänningsdatalagen hänvisar, genom 8 § första stycket 13, till dessa bestämmelser.

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) föreslagit en övergångsbestämmelse till dataskyddslagen som innebär att äldre föreskrifter fortfarande gäller för överklagande av beslut som har meddelats med stöd av dessa föreskrifter. Det framgår inte uttryckligen av Dataskyddsutredningens betänkande om övergångsbestämmelsen är tänkt att gälla samtliga typer av beslut som kan överklagas enligt personuppgiftslagen. Eftersom inget annat framgår anser vi dock att man får förutsätta att så är fallet.

Av skäl 171 till dataskyddsförordningen framgår 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, dvs. senast den 24 maj 2018.<sup>3</sup> Innebörden av detta är inte helt lättolkad; vid samordning med andra utredningar har frågan lyfts om skäl 171 utgör ett absolut hinder mot övergångsbestämmelser som innebär att äldre föreskrifter fortsatt ska gälla i vissa fall. Enligt vår mening innebär skäl 171 endast att de personuppgiftsansvariga måste ha

<sup>3</sup> Dataskyddsförordningen träder i kraft den tjugonde dagen efter det att den har offentliggjorts i Europeiska unionens officiella tidning, vilket skedde den 4 maj 2016. Förordningen börjar tillämpas den 25 maj 2018 (se artikel 99 i dataskyddsförordningen).

anpassat sin personuppgiftsbehandling till dataskyddsförordningens regelverk vid den tid då förordningen börjar tillämpas. Vi anser att skälet inte kan ges någon betydelse utöver detta, vilket innebär att det enligt vår bedömning inte utgör något hinder för övergångsbestämmelser som träffar den behandling av personuppgifter som har skett före det att dataskyddsförordningen börjar tillämpas.

Huvudprincipen när det gäller förvaltningsrättsliga föreskrifter är att de föreskrifter som är i kraft vid tidpunkten för prövningen av ett mål eller ärende ska ligga till grund för prövningen. Principen är emellertid inte undantagslös; bl.a. måste EU-rättslig praxis och förbudet mot retroaktiv tillämpning i 2 kap. 10 § RF beaktas. Undantag kan vidare följa av övergångsbestämmelser eller av uttalanden i motiven till lagstiftningen. För civilrättslig lagstiftning är utgångspunkten en annan; som regel träffar sådan lagstiftning inte rättshandlingar som har utförts innan lagstiftningen träder i kraft.<sup>4</sup>

Vi anser att man inte rimligen kan begära att de personuppgiftsansvariga ska utföra sin personuppgiftsbehandling i enlighet med dataskyddsförordningens regelverk även innan den ska börja tillämpas. Enligt vår mening är det därmed rimligt att handläggningen i domstol efter överklagande av beslut som fattats enligt det äldre regelverket sker enligt detta regelverk. Det faktum att det för dataskyddslagen ska finnas en övergångsbestämmelse med denna innebörd talar enligt vår mening vidare för att det även i utlänningsdatalagen bör införas en sådan bestämmelse. På detta sätt kan enhetlighet upprätthållas för samtliga överprövningar på området.

Det kan enligt vår mening inte heller uteslutas att det kan uppstå situationer där den registrerade skulle ha vunnit framgång med ett överklagande om det hade handlagts enligt äldre föreskrifter, men inte om det hade handlagts enligt bestämmelserna i dataskyddsförordningen och dess kompletterande regelverk. Utan en övergångsbestämmelse liknande den som föreslagits för dataskyddslagen skulle den registrerade i dessa fall göra en rättsförlust. Skulle situationen bli den motsatta – den registrerade skulle haft framgång med sitt överklagande om det handlagts enligt de nyare föreskrifterna men inte enligt de äldre – finns alltid möjligheten för

---

<sup>4</sup> Jfr RÅ 1996 ref. 57, med hänvisning till RÅ 1988 ref. 132.

den registrerade att på nytt framställa en begäran till den personuppgiftsansvarige och därmed få sin begäran bedömd utifrån det nya regelverket. Mot den bakgrunden föreslår vi att det till våra författningsförslag ska finnas en övergångsbestämmelse med innebörden att äldre föreskrifter fortfarande gäller för överklagande av beslut som har meddelats med stöd av de föreskrifterna. Övergångsbestämmelsen är avsedd att träffa beslut som meddelats av Datainspektionen och som kan överklagas enligt 51 § PuL samt de beslut de aktuella myndigheterna fattar i sin egenskap av personuppgiftsansvariga myndigheter och som kan överklagas enligt 52 § PuL.

## 20.4 Skada som har orsakats före ikraftträdandet

**Bedömning:** Det behövs inte några övergångsbestämmelser gällande skadestånd för skada som har orsakats före ikraftträdandet.

Utlänningsdatalagen hänvisar, genom 8 § första stycket 12, till 48 § PuL. Den sistnämnda bestämmelsen reglerar personuppgiftsansvarigas skadeståndsansvar om en behandling har utförts i strid med personuppgiftslagen.

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) föreslagit att det till dataskyddslagen ska finnas en övergångsbestämmelse som innebär att äldre föreskrifter om skadestånd fortfarande gäller för skada som har orsakats före ikraftträdandet.

Det faktum att utlänningsdatalagen hänvisar till bestämmelsen om skadeståndsansvar i 48 § PuL innebär enligt vår mening att en övergångsbestämmelse till dataskyddslagen som träffar den bestämmelsen även omfattar den rätt till skadestånd som en registrerad kan ha enligt utlänningsdatalagen. Redan av den anledningen anser vi att någon särskild övergångsbestämmelse för skadeståndsärenden inte behövs till våra författningsförslag.

Skulle en annan bedömning göras följer det också av allmänna principer att äldre bestämmelser gäller för ett anspråk om skadestånd som har uppkommit före det att nya bestämmelser

träder i kraft.<sup>5</sup> Oavsett vilken bedömning som görs anser vi därmed att det inte behövs någon övergångsbestämmelse till våra författningsförslag så vitt avser skadeståndsanspråk.

## 20.5 Sanktioner mot överträdelser som har skett före ikraftträdandet

**Bedömning:** Det behövs inte några övergångsbestämmelser gällande sanktioner mot överträdelser som har skett före ikraftträdandet.

Dataskyddsförordningen och Dataskyddsutredningens förslag till dataskyddslag innebär att systemet för sanktioner gentemot de personuppgiftsansvariga förändras. Den straffrättsliga reglering som finns i 49 § PuL kommer inte att ha någon motsvarighet i det nya regelverket. Inte heller kommer den möjlighet som nu finns för Datainspektionen att förena sina förelägganden med vite (44 och 45 §§ PuL) att finnas kvar.<sup>6</sup> I stället ska tillsynsmyndigheten, enligt artikel 83 i dataskyddsförordningen, under vissa förutsättningar besluta om administrativa sanktionsavgifter mot en personuppgiftsansvarig som har behandlat personuppgifter i strid med förordningens bestämmelser.

Vårt förslag innebär att dataskyddslagens bestämmelser om administrativa sanktionsavgifter mot myndigheter ska gälla även på utlänningsdatalagens tillämpningsområde. Regleringen ska genomföras genom en hänvisning i utlänningsdatalagen till de aktuella bestämmelserna i dataskyddslagen (se avsnitt 9.4.14). Personuppgiftslagens bestämmelser om vite och straff gäller för närvarande emellertid inte på utlänningsdatalagens tillämpningsområde. Detta innebär att det inte behövs någon övergångsbestämmelse som klargör vilket av sanktionssystemen – det gamla eller det nya – som ska tillämpas för överträdelser som skett före ikraftträdandet.

I 2 kap. 10 § RF finns ett förbud mot retroaktiv straff- och skattelagstiftning. Förbudet mot retroaktiv skattelag anses analogi-

<sup>5</sup> Jfr förarbetena till lagen (1987:667) om ekonomiska föreningar (prop. 2015/16:4 s. 205).

<sup>6</sup> Se Dataskyddsutredningens betänkande (SOU 2017:39 s. 294 ff.).

vis vara tillämpligt på straffliknande administrativa påföljder.<sup>7</sup> Mot den bakgrunden finns det enligt vår mening inte heller anledning att införa någon övergångsbestämmelse som reglerar att administrativa sanktionsavgifter inte får beslutas för överträdelse som skett innan våra författningsförslag träder i kraft.

---

<sup>7</sup> Se förarbetena till ändring i regeringsformen (prop. 1975/76:209 s. 125).



## 21 Konsekvenser av förslagen

### 21.1 Analysens omfattning och förslagens konsekvenser

**Bedömning:** Förslagen har inte någon påverkan på brottsligheten eller jämställdheten mellan män och kvinnor. Förslagen får inte någon betydelse för kommuner eller företag. De medför inte några samhällsekonomiska, sociala eller miljömässiga konsekvenser.

I vårt uppdrag ingår att belysa vilka konsekvenser de föreslagna ändringarna bedöms få. Om förslagen förväntas leda till kostnadsökningar för det allmänna, ska vi även föreslå hur dessa ska finansieras.

Dataskyddsförordningen kommer, när den börjar tillämpas, att innehålla de grundläggande bestämmelserna för de aktuella myndigheternas personuppgiftsbehandling. Vår konsekvensbedömning omfattar inte de förändringar i regelverket som följer direkt av dataskyddsförordningen eller som är en följd av förordningens tvingande bestämmelser. En sådan analys möter enligt vår mening oöverstigliga hinder; exempelvis har vi inte möjlighet att bedöma vilka anpassningar som eventuellt måste göras av befintliga datasystem för att de aktuella myndigheternas personuppgiftsbehandling ska vara förenlig med dataskyddsförordningens bestämmelser om dataskydd.

Det ligger enligt vår mening inte heller inom vårt uppdrag att bedöma konsekvenserna av att EU:s dataskyddsreform innebär att Polismyndigheten kommer att behöva förhålla sig till två regelverk för personuppgiftsbehandling; brottsdatalagen med tillhörande registerförfattning respektive dataskyddsförordningen med

tillhörande registerförfattningar samt – i tillämpliga delar – dataskyddslagen.

Vår analys kommer således endast att behandla konsekvenserna av de förslag som materiellt innebär en förändring gentemot nuvarande reglering och där det finns ett utrymme att nationellt bedöma vilken reglering som ska införas.

Med undantag för det som framgår i nästa avsnitt bedömer vi vidare att våra förslag inte innebär några konsekvenser för andra än de personuppgiftsansvariga myndigheterna. Förslagen får således inte någon betydelse för kommuner eller företag. Inte heller innebär de att några samhällsekonomiska konsekvenser uppstår. Det rör sig vidare främst om ett administrativt regelverk för personuppgiftsbehandling, som inte har några konsekvenser för brottsligheten eller det brottsförebyggande arbetet, sysselsättningen, miljön, offentlig service, jämställdhet eller möjligheterna att nå de integrationspolitiska målen.

## 21.2 Tillsynsmyndighetens handläggning och beslut samt sanktionsavgifter

**Bedömning:** De eventuella kostnader som uppstår för Migrationsverket, Polismyndigheten, utlandsmyndigheterna, tillsynsmyndigheten och de allmänna förvaltningsdomstolarna med anledning av våra förslag ryms inom befintliga anslag.

Vi har föreslagit att dataskyddslagens föreslagna bestämmelser om tillsynsmyndighetens handläggning och beslut ska gälla även på utlänningsdatalagens tillämpningsområde. Vissa av dessa bestämmelser är nyheter jämfört med den nuvarande regleringen. Det gäller möjligheten för tillsynsmyndigheten att under vissa speciella omständigheter väcka talan i domstol och möjligheten att överklaga domstolens avgörande i en sådan fråga (6 kap. 2 § och 8 kap. 6 § dataskyddslagen). Det gäller även rätten för den registrerade att i vissa fall begära besked från tillsynsmyndigheten angående ett tillsynsärende (6 kap. 5 § dataskyddslagen) och rätten till dröjsmålstalan mot tillsynsmyndighetens beslut i ett sådant ärende (8 kap. 3 § dataskyddslagen). Vårt förslag innebär också att dataskyddslagens bestämmelser om sanktionsavgifter mot

myndigheter ska gälla även på utlänningsdatalagens område (7 kap. 1, 3 och 4 §§ dataskyddslagen).

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39 s. 348 f.) gjort en bedömning av vilka konsekvenser de ovan nämnda bestämmelserna i dataskyddslagen kommer att få för tillsynsmyndigheten och för de allmänna förvaltningsdomstolar som har att pröva de aktuella målen. Dataskyddsutredningen menar att de ärenden och mål som blir följderna av denna reglering kommer att vara sparsamt förekommande. Det faktum att den generella regleringen kommer att gälla även inom utlänningsdatalagens tillämpningsområde bör enligt vår mening därmed medföra endast försumbara ytterligare kostnader för tillsynsmyndigheten och de allmänna förvaltningsdomstolarna. Dessa bör enligt vår mening rymmas inom befintliga budgetar. Vi uppskattar vidare att de föreslagna förändringarna i denna del inte bör föranleda några kostnader som inte rymms inom befintliga anslag för Migrationsverket, Polismyndigheten och utlandsmyndigheterna.



## 22 Författningskommentar

Vi har i föregående kapitel utförligt redogjort för de överväganden som ligger bakom de förändringar av utlänningsdatalagens bestämmelser som vi föreslår i denna promemoria. Av den anledningen är författningskommentarerna begränsade till att i huvudsak avse hänvisningar till de avsnitt i promemorian där respektive bestämmelse behandlas.

### **22.1 Förslaget till lag om ändring i utlänningsdatalagen (2016:27)**

#### *3 §*

*Denna lag gäller också vid behandling av personuppgifter i Polismyndighetens verksamhet som rör utlänningars inresa och vistelse i Sverige och utresa eller avlägsnande från Sverige.*

Paragrafen är ändrad. Förslaget behandlas i avsnitt 7.2.4.

#### *3 a §*

*Denna lag gäller inte vid sådan behandling av personuppgifter som omfattas av brottsdatalagens (2018:xx) tillämpningsområde.*

Paragrafen är ny. Förslaget behandlas i avsnitt 7.2.4.

## 5 §

*Denna lag gäller inte när personuppgifter behandlas med stöd av*

- 1. lagen (2000:344) om Schengens informationssystem,*
- 2. lagen (2006:444) om passagerarregister,*
- 3. Europaparlamentets och rådets förordning (EG) nr 810/2009 av den 13 juli 2009 om införande av en gemenskapskodex om viseringar (viseringskodex), eller*
- 4. Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodacuppgifter för brottsbekämpande ändamål, samt om ändring av förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (omarbetning).*

Paragrafen är ändrad genom att punkten 2 har tillkommit. Våra överväganden finns i avsnitt 7.3.2.

*Personuppgiftsbehandling enligt VIS-förordningen*

## 6 §

*När personuppgifter behandlas med stöd av Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS-förordningen) gäller, om inte något annat följer av VIS-förordningen, följande.*

- 1. Den personuppgiftsansvarige är skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med VIS-förordningen. Den personuppgiftsansvarige ska också underrätta tredje man till*

*vilken uppgifterna har lämnats ut om åtgärden, om den registrerade begär det eller om mera betydande skada eller olägenhet för den registrerade skulle kunna undvikas genom en underrättelse. Någon sådan underrättelse behöver dock inte lämnas, om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.*

*2. Den personuppgiftsansvarige ska ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med VIS-förordningen har orsakat. Ersättningskyldigheten kan i den utsträckning det är skäligt jämkas, om den personuppgiftsansvarige visar att felet inte berodde på honom eller henne.*

*I övrigt är denna lag inte tillämplig när personuppgifter behandlas med stöd av VIS-förordningen.*

Paragrafen är ändrad. Förslaget behandlas i avsnitt 7.3.3.

#### *Förhållandet till annan lagstiftning*

##### *6 a §*

*Denna lag innehåller kompletterande bestämmelser till 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 är ny. Förslaget behandlas i avsnitt 9.1 och 9.2.

##### *7 §*

*Om inte något annat anges i 8 §, gäller denna lag i stället för lagen (2018:xx) med kompletterande bestämmelser till EU:s dataskyddsförordning.*

Paragrafen är ändrad. Våra överväganden finns i avsnitt 9.3.

## 8 §

*När personuppgifter behandlas enligt denna lag, eller enligt föreskrifter som har meddelats i anslutning till lagen, gäller följande bestämmelser i lagen (2018:xx) med kompletterande bestämmelser till EU:s dataskyddsförordning:*

*1. 1 kap. 4 § första stycket om förhållandet till tryck- och yttrandefriheten,*

*2. 3 kap. 6 § första stycket om behandling av känsliga personuppgifter för arkivändamål av allmänt intresse,*

*3. 3 kap. 13 § om behandling av personnummer och samordningsnummer,*

*4. 4 kap. 1 § om användningsbegränsningar för arkiverade personuppgifter,*

*5. 5 kap. 1 § första stycket och 5 kap. 2 § om begränsningar av vissa rättigheter och skyldigheter,*

*6. 6 kap. 1–5 §§ om tillsynsmyndighetens handläggning och beslut,*

*7. 7 kap. 1, 3 och 4 §§ om administrativa sanktionsavgifter,*

*8. 8 kap. 1 § om skadestånd, och*

*9. 8 kap. 2–4 och 6 §§ om överklagande.*

Paragrafen är ändrad. Förslaget behandlas i avsnitt 9.1 och 9.3 vad gäller paragrafens ingress. I övrigt behandlas förslaget i avsnitt 9.4.13 (punkten 1), avsnitt 17.1.4 (punkten 2), avsnitt 9.4.4 (punkten 3), avsnitt 17.1.4 (punkten 4), avsnitt 14.3.3 och 14.5.3 (punkten 5), avsnitt 9.4.10 (punkten 6), avsnitt 9.4.14 (punkten 7), avsnitt 14.8.4 (punkten 8) och avsnitt 19.4 (punkten 9).

Det nuvarande andra stycket återfinns enligt vårt förslag i den nya 13 a § andra stycket. Förslaget finns i avsnitt 17.3.3. Det nuvarande tredje stycket föreslås utgå. Övervägandena i denna del finns i avsnitt 9.1.

## 13 §

*Personuppgifter som behandlas enligt 11 och 12 §§ får även behandlas när det är nödvändigt för att tillhandahålla information till*

*1. riksdagen eller regeringen,*

*2. en annan myndighet eller en enskild, om uppgifterna lämnas med stöd av lag eller förordning, eller*



*3. en utländsk myndighet, ett EU-organ eller en mellanfolklig organisation, om utlämnandet av uppgifterna följer av Sveriges medlemskap i Europeiska unionen eller av uppgiftsskyldighet enligt en internationell konvention som Sverige har tillträtt eller enligt ett av riksdagen godkänt avtal med främmande stat eller mellanfolklig organisation.*

*I ett enskilt fall får personuppgifter som behandlas enligt 11 och 12 §§ även behandlas för att tillhandahålla information för något annat ändamål än de som anges i första stycket under förutsättning att behandlingen är tillåten enligt artiklarna 5.1 b och 6.4 i Europaparlamentets och rådets förordning (EU) 2016/679.*

Paragrafens andra stycke är ändrat. Förslaget behandlas i avsnitt 8.6.

### 13 a §

*Personuppgifter som behandlas eller har behandlats enligt 11–12 §§ får även behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 i Europaparlamentets och rådets förordning (EU) 2016/679.*

*Första stycket gäller inte om personuppgifter ska gallras enligt denna lag, eller enligt föreskrifter som har meddelats i anslutning till lagen.*

Paragrafen är ny. Förslaget finns i avsnitt 17.1.4 vad gäller första stycket. Andra stycket finns i dag i 8 § andra stycket och våra överväganden i denna del finns i avsnitt 17.3.3.

### 15 §

*Sådana särskilda kategorier av uppgifter som anges i artikel 9.1 i Europaparlamentets och rådets förordning (EU) 2016/679 (känsliga personuppgifter) får endast behandlas*

*1. för de ändamål som anges i 11 § 1–4 och 6 samt 13 § om uppgifterna är absolut nödvändiga för syftet med behandlingen, eller*

*2. i löpande text för det ändamål som anges i 12 § 2, om uppgifterna är absolut nödvändiga för att fullgöra arbetsuppgifter i sådan verksamhet som anges i 2 §.*

*Vad som sägs i första stycket hindrar inte att känsliga personuppgifter behandlas med stöd av 15 a §.*

*Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela*

*1. ytterligare föreskrifter om inskränkningar av möjligheten att behandla känsliga personuppgifter, och*

*2. föreskrifter om gallring.*

Paragrafens första och andra stycke är ändrade. Våra överväganden finns i avsnitt 12.1.5.

### 17 §

*Vid sökning i personuppgifter är det förbjudet att använda sökbegrepp som avslöjar känsliga personuppgifter enligt 15 §.*

*Vad som sägs i första stycket hindrar inte att känsliga personuppgifter behandlas med stöd av 15 a §.*

Paragrafen är ändrad. Förslaget behandlas i avsnitt 12.2.2.

### 18 §

*Vid behandling av personuppgifter för ändamål som anges i 12 § 2 får personuppgifter som direkt pekar ut den registrerade inte användas som sökbegrepp.*

*Vid sökning i personuppgifter får uppgifter om lagöverträdelse som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden inte användas som sökbegrepp. Uppgifter om beslut om förvar enligt utlänningslagen (2005:716) får dock användas som sökbegrepp.*

Paragrafens andra stycke innehåller en redaktionell ändring. Förslaget finns i avsnitt 12.2.2.

*Begränsningar av vissa rättigheter och skyldigheter**18 a §*

*Bestämmelserna om den registrerades rätt att få information om en personuppgiftsincident enligt artikel 34 i Europaparlamentets och rådets förordning (EU) 2016/679, gäller inte om den personuppgiftsansvarige, enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning, inte får lämna ut uppgifter till den registrerade.*

Paragrafen är ny. Förslaget behandlas i avsnitt 14.9.2.

*20 §*

*Polismyndigheten har rätt att ta del av personuppgifter som Migrationsverket behandlar enligt 11 eller 15 a § vid direktåtkomst enligt 19 §. Säkerhetspolisen och utlandsmyndigheterna har motsvarande rätt att vid direktåtkomst ta del av uppgifter som Migrationsverket behandlar enligt 11 §.*

*Migrationsverket ska på begäran av Polismyndigheten, Säkerhetspolisen eller en utlandsmyndighet lämna ut personuppgifter som verket behandlar enligt 11 § 1 eller 2. Migrationsverket ska också på begäran av Polismyndigheten lämna ut personuppgifter som verket behandlar enligt 15 a § andra stycket 1, 2 eller 5.*

*Om det finns skäl för det ska Migrationsverket på eget initiativ lämna uppgifter som avses i andra stycket andra meningen till Polismyndigheten.*

Paragrafen innehåller redaktionella ändringar med anledning av att nuvarande 14 § utlänningsdatalagen föreslås återfinnas i den nya 15 a § samma lag. Förslaget behandlas i avsnitt 15.3.

*21 §*

*Personuppgifter får föras över till tredjeland även utan den registrerades samtycke om överföringen är absolut nödvändig för de*

*ändamål som anges i 11 § 1 och 2 samt 12 § 1, såvida det inte möter hinder av sekretess enligt offentlighets- och sekretesslagen (2009:400).*

*Sådan överföring får ske även om det inte finns något beslut om adekvat skyddsnivå enligt artikel 45.3 eller lämpliga skyddsåtgärder enligt artikel 46 i Europaparlamentets och rådets förordning (EU) 2016/679.*

*Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om begränsningar av möjligheten att föra över personuppgifter till tredjeland.*

Paragrafens första stycke innehåller en redaktionell ändring och dess andra stycke är nytt. Förslaget behandlas i avsnitt 16.3.

## 22.2 Förslaget till förordning om ändring i utlänningsdataförordningen (2016:30)

### 9 §

*Polismyndighetens direktåtkomst ska begränsas till de personuppgifter som myndigheten behöver för de ändamål som anges i 11 § 1–4 och 15 a § andra stycket 2 utlänningsdatalagen (2016:27).*

Paragrafen innehåller en redaktionell ändring med anledning av att nuvarande 14 § utlänningsdatalagen föreslås återfinnas i den nya 15 a § samma lag. Våra överväganden finns i avsnitt 15.3.



# Uppdraget

## **Anpassning av Kriminalvårdens personuppgiftsreglering och personuppgiftsregleringen i utlännings- och medborgarskapslagstiftningen till EU:s nya dataskyddsförordning – tilläggsuppdrag till Ju 2016:G**

### **Uppdraget**

Utredaren ges i uppdrag att även lämna förslag på de författningsändringar som behövs för att komplettera EU:s dataskyddsförordning ([EU] 2016/679) i utlänningsdatalagen (2016:27), utlänningsdataförordningen (2016:30) och när det gäller Kriminalvårdens personuppgiftsbehandling. I uppdraget ingår inte att se över författningarna med anledning av det nya dataskyddsdirektivet ([EU] 2016/680).

Uppdraget förlängs och ska redovisas senast den 30 september 2017.

### **Bakgrund**

Justitiedepartementet har den 7 september 2016 gett en utredare i uppdrag att lämna förslag på de författningsändringar som behövs i domstolsdatalagen (2015:728) och domstolsdataförordningen (2015:729) med anledning av dataskyddsförordningen. Uppdraget ska redovisas senast den 8 maj 2017 (Ju 2016:G).

## Behovet av ett tilläggsuppdrag

### *Kriminalvården*

Kriminalvården har i uppdrag att verkställa utdömda fängelsestraff och icke frihetsberövande påföljder, bedriva häktesverksamhet och utföra transporter. Behandlingen av personuppgifter i den verksamheten regleras i lagen (2001:617) om behandling av personuppgifter inom kriminalvården som kompletteras av förordningen (2001:682) om behandling av personuppgifter inom kriminalvården. Av lagen följer också att personuppgiftslagen (1998:204) ska tillämpas vid behandling av personuppgifter inom kriminalvården om inte annat följer av lagen eller föreskrifter som har meddelats med stöd av lagen.

Det avgörande för om en viss personuppgiftsbehandling kommer att omfattas av dataskyddsförordningen eller det nya dataskyddsdirektivet kommer att vara i vilket syfte uppgifterna behandlas. Dataskyddsdirektivet är bl.a. tillämpligt på behöriga myndigheters behandling av personuppgifter för att verkställa straffrättsliga påföljder. Den del av Kriminalvårdens verksamhet som avser verkställighet av påföljd kommer således att omfattas av det nya dataskyddsdirektivets tillämpningsområde. Lagen respektive förordningen om behandling av personuppgifter inom kriminalvården reglerar till allra största delen den personuppgiftsbehandling som krävs för verksamhet under dataskyddsdirektivets tillämpningsområde. Det rör sig huvudsakligen om personuppgiftsbehandling för verkställighet av straff, häktesverksamhet och personutredning i brottmål. När personuppgifter behandlas i de delar av verksamheten som inte faller in under verkställighet av påföljd eller något av de andra syften som räknas upp i direktivet kommer Kriminalvården att behöva tillämpa dataskyddsförordningen. Det kan därutöver finnas verksamhet som faller utanför EU-rättens tillämpningsområde.

I det uppdrag som Utredningen om 2016 års dataskyddsdirektiv (dir. 2016:21) har ingår att analysera och bedöma behovet av författningsändringar för att anpassa bl.a. lagen om behandling av personuppgifter inom kriminalvården till direktivets förpliktelser och de nya förutsättningarna för regleringen. I Dataskyddsutredningens (dir. 2016:15) uppdrag ingår inte att se över eller



lämna förslag om behandling av personuppgifter i olika myndigheters verksamhet. Det finns därför ett behov av en närmare analys av vilka bestämmelser som behövs för att komplettera dataskyddsförordningens bestämmelser i regleringen av Kriminalvårdens hantering av personuppgifter.

### *Verksamhet enligt utlännings- och medborgarskapslagstiftningen*

Migrationsverket, Polismyndigheten, Säkerhetspolisen och utlandsmyndigheterna bedriver verksamhet enligt utlännings- och medborgarskapslagstiftningen. Behandlingen av personuppgifter i sådan verksamhet regleras i utlänningsdatalagen som kompletteras av utlänningsdataförordningen. Av utlänningsdatalagen följer att den som huvudregel gäller i stället för personuppgiftslagen.

I Dataskyddsutredningens uppdrag ingår inte att se över eller lämna förslag på ändringar i utlänningsdatalagen eller utlänningsdataförordningen. Det finns därför ett behov av en närmare analys av vilka bestämmelser som behövs för att komplettera dataskyddsförordningens bestämmelser i utlänningsdatalagen och utlänningsdataförordningen.

### **Närmare om uppdraget**

Utredaren ges i uppdrag att även lämna förslag på de författningsändringar som behövs för att komplettera EU:s dataskyddsförordning i utlänningsdatalagen, utlänningsdataförordningen och när det gäller Kriminalvårdens personuppgiftsbehandling. I uppdraget ingår inte att se över författningarna med anledning av det nya dataskyddsdirektivet.

Utredaren är fri att ta upp och lämna förslag i närliggande frågor som aktualiseras under utredningsuppdraget.

Utredaren ska belysa vilka konsekvenser de föreslagna ändringarna bedöms få. Om förslagen förväntas leda till kostnadsökningar för det allmänna, ska utredningen föreslå hur dessa ska finansieras.

Under utförandet av uppdraget ska utredaren följa och i lämplig omfattning samråda med andra utredningar som fått i uppdrag att anpassa svensk rätt till EU:s nya dataskyddsregelverk. Utredaren

ska också samråda med Kriminalvården, Migrationsverket och Polismyndigheten och vid behov inhämta synpunkter från övriga myndigheter som berörs.

Uppdraget förlängs och ska redovisas senast den 30 september 2017.

(Justitiedepartementet)

# Konsoliderad version av utlänningsdatalogen enligt våra förslag

I syfte att underlätta för läsaren åskådliggör vi i denna bilaga hur utlänningsdatalogen kommer att se ut i sin helhet om samtliga förslag i denna promemoria leder till lagstiftning. Vi har dock exkluderat både befintliga och föreslagna ikraftträdande- och övergångsbestämmelser. Eftersom vi endast föreslår mindre redaktionella ändringar av utlänningsdataförordningen finns det enligt vår mening inte samma behov av att återge den förordningen här.

## Utlänningsdatalogen (2016:27)

### 1 §

Syftet med denna lag är att ge Migrationsverket, Polismyndigheten och utlandsmyndigheterna möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sin verksamhet enligt utlännings- och medborgarskapslagstiftningen och att skydda människor mot att deras personliga integritet kränks vid sådan behandling.

### *Lagens tillämpningsområde*

### 2 §

Denna lag gäller vid behandling av personuppgifter i Migrationsverkets och utlandsmyndigheternas verksamhet som rör

1. utlänningars inresa i Sverige, i en stat som ingår i Europeiska unionen, i en stat som är ansluten till Europeiska ekonomiska samarbetsområdet eller i Schweiz,

2. utlänningars vistelse eller arbete i Sverige och utresa eller avlägsnande från Sverige,
3. statusförklaring,
4. mottagande av asylsökande och andra utlänningar,
5. bistånd och stöd till utlänningar,
6. svenskt medborgarskap,
7. statlig ersättning för kostnader för utlänningar,
8. bosättning av utlänningar, eller
9. utfärdande av resehandlingar.

### 3 §

Denna lag gäller också vid behandling av personuppgifter i Polismyndighetens verksamhet som rör utlänningars inresa och vistelse i Sverige och utresa eller avlägsnande från Sverige.

### 3 a §

Denna lag gäller inte vid sådan behandling av personuppgifter som omfattas av brottsdatalagens (2018:xx) tillämpningsområde.

### 4 §

Lagen gäller endast om behandlingen av personuppgifter enligt 2 eller 3 § är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

### 5 §

Denna lag gäller inte när personuppgifter behandlas med stöd av

1. lagen (2000:344) om Schengens informationssystem,
2. lagen (2006:444) om passagerarregister,
3. Europaparlamentets och rådets förordning (EG) nr 810/2009 av den 13 juli 2009 om införande av en gemenskapskodex om viseringar (viseringskodex), eller
4. Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en

statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodacuppgifter för brottsbekämpande ändamål, samt om ändring av förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (omarbetning).

*Personuppgiftsbehandling enligt VIS-förordningen*

6 §

När personuppgifter behandlas med stöd av Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS-förordningen) gäller, om inte något annat följer av VIS-förordningen, följande.

1. Den personuppgiftsansvarige är skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med VIS-förordningen. Den personuppgiftsansvarige ska också underrätta tredje man till vilken uppgifterna har lämnats ut om åtgärden, om den registrerade begär det eller om mera betydande skada eller olägenhet för den registrerade skulle kunna undvikas genom en underrättelse. Någon sådan underrättelse behöver dock inte lämnas, om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

2. Den personuppgiftsansvarige ska ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med VIS-förordningen har orsakat. Ersättningsskyldigheten kan i den utsträckning det är skäligt jämkas, om den personuppgiftsansvarige visar att felet inte berodde på honom eller henne.

I övrigt är denna lag inte tillämplig när personuppgifter behandlas med stöd av VIS-förordningen.

*Förhållandet till annan lagstiftning*

## 6 a §

Denna lag innehåller kompletterande bestämmelser till 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).

## 7 §

Om inte något annat anges i 8 §, gäller denna lag i stället för lagen (2018:xx) med kompletterande bestämmelser till EU:s dataskyddsförordning.

## 8 §

När personuppgifter behandlas enligt denna lag, eller enligt föreskrifter som har meddelats i anslutning till lagen, gäller följande bestämmelser i lagen (2018:xx) med kompletterande bestämmelser till EU:s dataskyddsförordning:

1. 1 kap. 4 § första stycket om förhållandet till tryck- och yttrandefriheten,

2. 3 kap. 6 § första stycket om behandling av känsliga personuppgifter för arkivändamål av allmänt intresse,

3. 3 kap. 13 § om behandling av personnummer och samordningsnummer,

4. 4 kap. 1 § om användningsbegränsningar för arkiverade personuppgifter,

5. 5 kap. 1 § första stycket och 5 kap. 2 § om begränsningar av vissa rättigheter och skyldigheter,

6. 6 kap. 1–5 §§ om tillsynsmyndighetens handläggning och beslut,

7. 7 kap. 1, 3 och 4 §§ om administrativa sanktionsavgifter,

8. 8 kap. 1 § om skadestånd, och

9. 8 kap. 2–4 och 6 §§ om överklagande.

*Personuppgiftsansvar*

## 9 §

Migrationsverket, Polismyndigheten och en utlandsmyndighet är var och en personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför. Migrationsverket är dock personuppgiftsansvarigt för utlandsmyndigheternas automatiserade behandling av personuppgifter.

## 10 §

Upphävd genom SFS 2018:xx.

*Ändamål*

## 11 §

Migrationsverket, Polismyndigheten och utlandsmyndigheterna får behandla personuppgifter om det behövs för

1. handläggning av ärenden eller en myndighets biträde i sådana ärenden i verksamhet som avses i 2 och 3 §§,
2. kontroll av utlänning i samband med inresa och utresa samt kontroll under vistelsen i Sverige,
3. utförande av arbetsuppgifter som gäller mottagande och bosättning av asylsökande och andra utlänningar,
4. framställning av statistik,
5. utförande av testverksamhet, eller
6. fullgörande av en rättslig skyldighet att registrera eller på annat sätt dokumentera en personuppgift.

## 12 §

Migrationsverket får också behandla personuppgifter om det behövs för återsökning av

1. avgöranden, rättsutredningar och annan rättslig information, eller
2. information som rör förhållanden i andra länder.

## 13 §

Personuppgifter som behandlas enligt 11 och 12 §§ får även behandlas när det är nödvändigt för att tillhandahålla information till

1. riksdagen eller regeringen,
2. en annan myndighet eller en enskild, om uppgifterna lämnas med stöd av lag eller förordning, eller
3. en utländsk myndighet, ett EU-organ eller en mellanfolklig organisation, om utlämnandet av uppgifterna följer av Sveriges medlemskap i Europeiska unionen eller av uppgiftsskyldighet enligt en internationell konvention som Sverige har tillträtt eller enligt ett av riksdagen godkänt avtal med främmande stat eller mellanfolklig organisation.

I ett enskilt fall får personuppgifter som behandlas enligt 11 och 12 §§ även behandlas för att tillhandahålla information för något annat ändamål än de som anges i första stycket under förutsättning att behandlingen är tillåten enligt artiklarna 5.1 b och 6.4 i Europaparlamentets och rådets förordning (EU) 2016/679.

#### 13 a §

Personuppgifter som behandlas eller har behandlats enligt 11–12 §§ får även behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 i Europaparlamentets och rådets förordning (EU) 2016/679.

Första stycket gäller inte om personuppgifter ska gallras enligt denna lag, eller enligt föreskrifter som har meddelats i anslutning till lagen.

#### 14 §

Upphävd genom SFS 2018:xx.

#### *Behandling av känsliga personuppgifter*

#### 15 §

Sådana särskilda kategorier av uppgifter som anges i artikel 9.1 i Europaparlamentets och rådets förordning (EU) 2016/679 (känsliga personuppgifter) får endast behandlas

1. för de ändamål som anges i 11 § 1–4 och 6 samt 13 § om uppgifterna är absolut nödvändiga för syftet med behandlingen, eller



2. i löpande text för det ändamål som anges i 12 § 2, om uppgifterna är absolut nödvändiga för att fullgöra arbetsuppgifter i sådan verksamhet som anges i 2 §.

Vad som sägs i första stycket hindrar inte att känsliga personuppgifter behandlas med stöd av 15 a §.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela

1. ytterligare föreskrifter om inskränkningar av möjligheten att behandla känsliga personuppgifter, och

2. föreskrifter om gallring.

### *Migrationsverkets register över fingeravtryck och fotografier*

#### 15 a §

Migrationsverket får föra separata register över fingeravtryck och fotografier som tas med stöd av 9 kap. 8 § utlänningslagen (2005:716).

Med begränsning av de ändamål som annars gäller enligt 11 och 13 §§ får uppgifter om fingeravtryck eller fotografier i registren användas endast

1. vid prövning av ansökningar om uppehållstillstånd där skäl som anges i 4 kap. 1–2 a §§ utlänningslagen åberopas,

2. i ärenden om avvisning och utvisning,

3. i testverksamhet,

4. om det behövs för att kontrollera identiteten av en person på ett fotografi som kommit in till Migrationsverket, eller

5. om det behövs för att Migrationsverket ska kunna kontrollera ett fingeravtryck mot det fingeravtrycks- och signalementsregister som Polismyndigheten för enligt 4 kap. 11 § polisdatalagen (2010:361).

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela

1. ytterligare föreskrifter om vilka uppgifter som får behandlas i registren över fingeravtryck och fotografier, och

2. föreskrifter om gallring.

### *Tillgången till personuppgifter*

#### 16 §

Tillgången till personuppgifter ska begränsas till det som varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om tillgången till personuppgifter.

### *Sökbegränsningar*

#### 17 §

Vid sökning i personuppgifter är det förbjudet att använda sökbegrepp som avslöjar känsliga personuppgifter enligt 15 §.

Vad som sägs i första stycket hindrar inte att känsliga personuppgifter behandlas med stöd av 15 a §.

#### 18 §

Vid behandling av personuppgifter för ändamål som anges i 12 § 2 får personuppgifter som direkt pekar ut den registrerade inte användas som sökbegrepp.

Vid sökning i personuppgifter får uppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden inte användas som sökbegrepp. Uppgifter om beslut om förvar enligt utlänningslagen (2005:716) får dock användas som sökbegrepp.

### *Begränsningar av vissa rättigheter och skyldigheter*

#### 18 a §

Bestämmelserna om den registrerades rätt att få information om en personuppgiftsincident enligt artikel 34 i Europaparlamentets och rådets förordning (EU) 2016/679, gäller inte om den personuppgiftsansvarige, enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning, inte får lämna ut uppgifter till den registrerade.

### *Direktåtkomst*

#### 19 §

Direktåtkomst till personuppgifter hos Migrationsverket får endast medges

1. Polismyndigheten,
2. Säkerhetspolisen,

3. utlandsmyndigheterna,

4. Försäkringskassan,

5. Pensionsmyndigheten,

6. Skatteverket, eller

7. en part eller en parts ombud eller biträde.

Direktåtkomst enligt första stycket 7 får endast avse personuppgifter i partens ärende.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela

1. ytterligare föreskrifter om begränsningar av direktåtkomst enligt första stycket, och

2. föreskrifter om behörighet och säkerhet vid sådan åtkomst.

### *Uppgiftsskyldighet*

#### 20 §

Polismyndigheten har rätt att ta del av personuppgifter som Migrationsverket behandlar enligt 11 eller 15 a § vid direktåtkomst enligt 19 §. Säkerhetspolisen och utlandsmyndigheterna har motsvarande rätt att vid direktåtkomst ta del av uppgifter som Migrationsverket behandlar enligt 11 §.

Migrationsverket ska på begäran av Polismyndigheten, Säkerhetspolisen eller en utlandsmyndighet lämna ut personuppgifter som verket behandlar enligt 11 § 1 eller 2. Migrationsverket ska också på begäran av Polismyndigheten lämna ut personuppgifter som verket behandlar enligt 15 a § andra stycket 1, 2 eller 5.

Om det finns skäl för det ska Migrationsverket på eget initiativ lämna uppgifter som avses i andra stycket andra meningen till Polismyndigheten.

### *Överföring av personuppgifter till tredjeland*

#### 21 §

Personuppgifter får föras över till tredjeland även utan den registrerades samtycke om överföringen är absolut nödvändig för de ändamål som anges i 11 § 1 och 2 samt 12 § 1, såvida det inte möter hinder av sekretess enligt offentlighets- och sekretesslagen (2009:400).

Sådan överföring får ske även om det inte finns något beslut om adekvat skyddsnivå enligt artikel 45.3 eller lämpliga skyddsåtgärder enligt artikel 46 i Europaparlamentets och rådets förordning (EU) 2016/679.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om begränsningar av möjligheten att föra över personuppgifter till tredjeland.

#### *Avskiljande*

##### 22 §

Personuppgifter som har behandlats för ändamål som anges i 11 § 1–4 och 13 § ska avskiljas så att tillgången till dem begränsas om de inte längre behövs i myndighetens löpande verksamhet.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om avskiljande av personuppgifter.

#### *Säkerhetsåtgärder*

##### 23 §

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om säkerhetsåtgärder till skydd för personuppgifter.

## 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 <sup>(1)</sup>,med beaktande av Regionkommitténs yttrande <sup>(2)</sup>,i enlighet med det ordinarie lagstiftningsförfarandet <sup>(3)</sup>, 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 <sup>(4)</sup> 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.

<sup>(1)</sup> EUT C 229, 31.7.2012, s. 90.

<sup>(2)</sup> EUT C 391, 18.12.2012, s. 127.

<sup>(3)</sup> 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.

<sup>(4)</sup> 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 (EGT L 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 fastställs 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 snedvrida 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 sektorspecifika 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 personuppgiftsansvariga 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<sup>(1)</sup>.
- (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 tekniskt neutralt 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<sup>(2)</sup> 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

<sup>(1)</sup> 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).

<sup>(2)</sup> 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<sup>(1)</sup>. 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 rättskipande 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<sup>(2)</sup>, 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 eller 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.

<sup>(1)</sup> 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).

<sup>(2)</sup> Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informations-samhällets tjänster, särskilt elektronisk handel, på den inre marknaden ("Direktiv om elektronisk handel") (EGT 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, personuppgiftsbiträdets 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 folkrätt, 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 nätidentifikatorer som lämnas av deras utrustning, applikationer, verktyg och protokoll, t.ex. ip-adresser, kakor eller andra identifikatorer, som radiofrekvensetiketter. Detta kan efterlämna spår som, särskilt i kombination med unika identifikatorer 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 ortvetydigt 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 betedande som i sammanhanget tydligt visar att den registrerade godtar den avsedda behandlingen av sina personuppgifter. Tyystnad, 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 innebär 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<sup>(1)</sup>, 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, sjukdomsrisik, 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

<sup>(1)</sup> 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 personuppgiftsbiträdet 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 personuppgiftsbiträdet 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 samlas in, 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 fastställs 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<sup>(1)</sup> 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 oskäliga 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 ojämlighet 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

<sup>(1)</sup> Rådets direktiv 93/13/EEG av den 5 april 1993 om oskäliga villkor i konsumentavtal (EGT L 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. Sådan 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 informations säkerhet, 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 samhällen 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 hälsovärdmyndigheter 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<sup>(1)</sup>, nämligen 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. 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 riktas 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.

<sup>(1)</sup> Europaparlamentets och rådets förordning (EG) nr 1338/2008 av den 16 december 2008 om gemenskapsstatistik om folkhälsa och hälsa och säkerhet i arbetet (EUT L 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 personuppgiftsbehandlings 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 nätidentifikatorer. 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 förhållandet 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 uppmanas 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 dataskyddstyrelsen 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 människa, 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 överträdelse 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 personuppgiftsansvarige 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 dataskyddsombud. 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 uppmannas 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 stor omfattning 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 sörga 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 anför behandling åt ett personuppgiftsbiträde, endast använda personuppgiftsbiträden 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 personuppgiftsbiträdena föra register över behandling som sker under deras ansvar. Alla personuppgiftsansvariga och personuppgiftsbiträden bör vara skyldiga att samarbeta med tillsynsmyndigheten och på dennes 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 personuppgiftsbiträden 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 överförs, lagrats eller på annat sätt behandlats, framför allt när denna kan medföra fysisk, materiell eller immateriell skada.
- (84) I syfte att sörga 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 fördörjningen 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 fortlöpande 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 anmälningskyldigheter 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, biometrisk 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 dataskyddsombud 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 uppmuntras 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 uppmuntras, 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 skäligen 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 dataskyddsovervakning och sörja för samarbetsmekanismer med medlemsstaternas dataskyddsmyndigheter, och de registrerade bör tillförsäkra effektiva och lagstaddade 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 tillägsprotokoll 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 (\*), 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

(\*) 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, finanstillsynsmyndigheter, 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 utnännas 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 personuppgiftsbiträdets 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 innebära 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 personuppgiftsbiträdes 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 personuppgiftsbiträdets 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 personuppgiftsbiträdets 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 personuppgiftsbiträdets 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 överträdelse 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 personuppgiftsbiträdets behandling men den sakfråga som klagomålet gäller eller den möjliga överträdelsen endast rör den personuppgiftsansvariges eller personuppgiftsbiträdets 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 personuppgiftsbiträden, 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 stadsegenliga 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 besluten 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 meddela 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 överträdelse 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 genomförandeakter 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<sup>(1)</sup>, påverka tillämpningen av sådana särskilda bestämmelser.
- (148) För att stärka verkställigheten av denna förordning bör det utdömas sanktioner, inbegripet administrativa sanktionsavgifter, för överträdelse 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 uppsåtligt, vilka åtgärder som vidtagits för att lindra skadan, graden av ansvar eller eventuella tidigare överträdelse 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 försvarande 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 överträdelse av denna förordning, inbegripet för överträdelse 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 överträdelse av denna förordning. Utdömandet av straffrättsliga påföljder för överträdelse 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 överträdelse av denna förordning bör samtliga tillsynsmyndigheter ha befogenhet att utfärda administrativa sanktionsavgifter. Det bör i denna

<sup>(1)</sup> Europaparlamentets och rådets förordning (EU) nr 1215/2012 av den 12 december 2012 om domstols behörighet och erkännande och verkställighet av domar på privaträttsområdet (EUT L 351, 20.12.2012, s. 1).

förordning anges vilka överträdelse 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 överträdelse 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 sammanjämningen 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 (\*) ska inte på något sätt påverka skyddsnivån för fysiska personer med avseende

(\*) 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 förenligt 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 förenligt 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 betedande 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 (\*) 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 (†) innehåller ytterligare preciseringar om statistisk konfidentialitet för europeisk statistik.
- (164) Vad beträffar tillsynsmyndigheternas befogenheter att från personuppgiftsansvariga eller personuppgiftsbiträden få tillgång till personuppgifter och tillräde 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

(\*) 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).

(†) 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 insynskyddade 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 uttalande den 7 mars 2012 <sup>(1)</sup>.
- (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 <sup>(2)</sup>, 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.

<sup>(1)</sup> EUT C 192, 30.6.2012, s. 7.

<sup>(2)</sup> 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 mellanhanders 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. *samttycke* av den registrerade: 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,
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 <sup>(1)</sup>,
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**

1. 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*).

<sup>(1)</sup> 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 föräldransvar 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 eftersträfvade 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 överträdelse

Behandling av personuppgifter som rör fällande domar i brottmål och överträdelse 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 begärs, 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 begränsningar 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 försämrar 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 allmänt intresse 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 tillhandahållit 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 informations-samhällets 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 överträdelse 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 utövat 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 överträdelser, 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 personuppgiftsbiträdet uppdrag, utöver eller i stället för den personuppgiftsansvarige eller personuppgiftsbiträdet, 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 personuppgiftsbiträdet utser en företrädare ska inte påverka de rättsliga åtgärder som skulle kunna inledas mot den personuppgiftsansvarige eller personuppgiftsbiträdet.

#### 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. Personuppgiftsbiträdet får inte anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhållande har erhållits av den personuppgiftsansvarige. Om ett allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbiträdet 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 personuppgiftsbiträdet 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 personuppgiftsbiträdet
  - 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 personuppgiftsbiträdet omfattas av, och i så fall ska personuppgiftsbiträdet 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 anlita 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 personuppgiftsbiträdet har att tillgå,
  - 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 utförs under dess ansvar. Detta register ska innehålla samtliga följande uppgifter:

- Namn och kontaktuppgifter för den personuppgiftsansvarige, samt i tillämpliga fall gemensamt personuppgiftsansvariga, den personuppgiftsansvariges företrädare samt dataskyddsombudet.
- Ändamålen med behandlingen.
- 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 tredjeländ eller en internationell organisation, inbegripet identifiering av tredjeländ 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 personuppgiftsbiträdets företrädare samt dataskyddsombudet.
- b) De kategorier av behandling som har utförts för varje personuppgiftsansvariges räkning.
- c) I tillämpliga fall, överföringar av personuppgifter till ett tredjeländ eller en internationell organisation, inbegripet identifiering av tredjeländ 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 personuppgiftsbiträdets 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 överförs, 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 utnännas 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 dataskyddsombudet 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 uppgiftsdataskyddsombudet 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. Dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbitrådets högsta förvaltningsnivå.
4. Den registrerade får kontakta dataskyddsombudet med avseende på alla frågor som rör behandlingen av dennes personuppgifter och utövatandet av dennes rättigheter enligt denna förordning.
5. Dataskyddsombudet ska, när det gäller dennes genomförande av sina uppgifter, vara bundet av sekretess eller konfidentialitet i enlighet med unionsrätten eller medlemsstaternas nationella rätt.
6. Dataskyddsombudet 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

#### Dataskyddsombudets uppgifter

1. Dataskyddsombudet 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 ansvarstildelning, 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. Dataskyddsombudet 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 personuppgiftsbiträden 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 förenlig 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 samlar 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 överträdelse 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 iaktas 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 personuppgiftsbiträdets 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 <sup>(1)</sup> i enlighet med EN-ISO/IEC 17065/2012 och med de ytterligare krav som fastställs 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,

<sup>(1)</sup> 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 upphåvande av förordning (EEG) nr 339/93 (EUT L 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 överträdelse 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 personuppgiftsbiträdes 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 tredjlandet 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 upphävs 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 upphävs 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 upphävs 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 dataskyddombud 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 tredjeland 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 tredjeland 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 anförtröts 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 utnämnas 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 lagsiftningsåtgärder 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 personuppgiftsbiträdets 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. Utövat 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. Utövat 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 meningen får 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

#### Tvistlösning 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 skyldigt 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 samrådsförandet.

#### 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 <sup>(1)</sup>.

## 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.

<sup>(1)</sup> 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 uppgiftsbehandlingsens karaktär, omfattning eller syfte samt antalet berörda registrerade och den skada som de har lidit.
  - b) Om överträdelsen skett med uppsåt eller genom oaksamhet.
  - 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 försvärande 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 oaksamhet 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 iaktas. 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 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 informationssamhället.

## 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.

L 119/88

SV

Europeiska unionens officiella tidning

4.5.2016

---

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*

---

# Departementsserien 2017

## Kronologisk förteckning

---

1. Elektronisk övervakning av kontaktförbud. Ju.
2. Åldersdifferentierat underhållsstöd och höjt grundavdrag för bidragsskyldiga föräldrar. S.
3. Genomförande av ICT-direktivet. Ju.
4. Sjukpenning i avvaktan på slutligt beslut. S.
5. Effektivare sanktioner i livsmedelskedjan m.m. N.
6. Förslag till lag om ersättning till personer som har fått ändrad könstillhörighet fastställd i vissa fall. S.
7. Kommunikation för vår gemensamma säkerhet. Uppdrag om en utvecklad och säker kommunikationslösning för aktörer inom allmän ordning, säkerhet, hälsa och försvar. Ju.
8. Kultursamverkan för ett Sverige som håller ihop. Framtida inriktning och utvecklingsmöjligheter för kultursamverkansmodellen. Ku.
9. Förstärkt rehabilitering för återgång i arbete. S.
10. ILO:s konvention om anständiga arbetsvillkor för hushållsarbetare. A.
11. Ändrade regler om retroaktivitet avseende efterlevandestöd. S.
12. Om förenklat beslutsfattande och särskilda boendeformer för äldre. S.
13. Skadeståndets bestämmande vid finansiell rådgivning. Fi.
14. Vissa ändringar i läkemedelslagen. S.
15. Ökat konsulärt skydd för unionsmedborgare och deras familjemedlemmar. Genomförande av direktiv (EU) 2015/637. UD.
16. Arbetsplatsinspektioner och höjd särskild avgift. Ju.
17. En ny lag om försäkringsdistribution. Fi.
18. Karensavdrag – en mer rättvis självrisk. S.
19. Anpassningar av de fastighetsrättsliga, associationsrättsliga, transporträttsliga och immaterialrättsliga författningarna till dataskyddsförordningen. Ju.
20. Regionalt utvecklingsansvar i Stockholms, Kalmar och Blekinge län. Fi.
21. Skyldighet för vissa offentliga funktionärer att anmäla innehav av finansiella instrument. Fi.
22. Utstationering och vägtransporter. A.
23. Kompletterande bestämmelser till EU:s förordning om personlig skyddsutrustning. Fi.
24. Skjutvapen och explosiva varor – Skärpta straff för de grova brotten. Ju.
25. Nya ungdomspåföljder. Ju.
26. En anpassning till dataskyddsförordningen – kreditupplysningslagen och några andra författningar. Ju.
27. Genomförande av säsongsanställningsdirektivet. Ju.
28. En anpassning till dataskyddsförordningen av dataskyddsbestämmelser inom Näringsdepartementets verksamhetsområde. N.
29. Utökade möjligheter till utbyte av läkemedel. S.
30. Ett entreprenörsansvar i bygg- och anläggningsbranschen. A.
31. Elektroniska fakturor vid offentlig upphandling. Fi.
32. Biologiskt mångfald och ekosystemtjänster. Kontrollstation 2016. M.
33. Anpassningar till dataskyddsförordningen av registerförfattningar inom Arbetsmarknadsdepartementets ansvarsområde. A.
34. Ändringar i bestämmelser om val till Sametinget. K.
35. Körkortslån. A.
36. En snabbare lagföring. Försöksprojekt med ett snabbförfarande i brottmål. Ju.

37. Frekventa och omfattande ärenden om utlämnande av allmän handling. Ju.
38. Livstidsstraff för mord. Ju.
39. Legitimation för hälso- och sjukvårdskuratorer. S.
40. Ändringar i vissa författningar inom Finansdepartementets ansvarsområde med anledning av EU:s dataskyddsreform. Fi.
41. En omarbetad domstolsdatalag. Anpassning till EU:s dataskyddsförordning. Ju.
42. Följdändringar till ny förvaltningslag. Ju.
43. Konsultation i frågor som rör det samiska folket. Ku.
44. Elmarknadslag. M.
45. En omarbetad utlänningsdatalag. Anpassning till EU:s dataskyddsförordning. Ju.

# Departementsserien 2017

---

## Systematisk förteckning

---

### Arbetsmarknadsdepartementet

- ILO:s konvention om anständiga arbetsvillkor för hushållsarbetare. [10]
- Utstationering och vägtransporter. [22]
- Ett entreprenörsansvar i bygg- och anläggningsbranschen. [30]
- Anpassningar till dataskyddsförordningen av registerförfattningar inom Arbetsmarknadsdepartementets ansvarsområde. [33]
- Körkortslån. [35]

### Finansdepartementet

- Skadeståndets bestämmande vid finansiell rådgivning. [13]
- En ny lag om försäkringsdistribution. [17]
- Regionalt utvecklingsansvar i Stockholms, Kalmar och Blekinge län. [20]
- Skyldighet för vissa offentliga funktionärer att anmäla innehav av finansiella instrument. [21]
- Kompletterande bestämmelser till EU:s förordning om personlig skyddsutrustning. [23]
- Elektroniska fakturor vid offentlig upphandling. [31]
- Ändringar i vissa författningar inom Finansdepartementets ansvarsområde med anledning av EU:s dataskyddsreform. [40]

### Justitiedepartementet

- Elektronisk övervakning av kontaktförbud. [1]
- Genomförande av ICT-direktivet. [3]
- Kommunikation för vår gemensamma säkerhet. Uppdrag om en utvecklad och säker kommunikationslösning för aktörer inom allmän ordning, säkerhet, hälsa och försvar. [7]
- Arbetsplatsinspektioner och höjd särskild avgift. [16]

- Anpassningar av de fastighetsrättsliga, associationsrättsliga, transporträttsliga och immaterialrättsliga författningarna till dataskyddsförordningen. [19]
- Skjutvapen och explosiva varor – Skärpta straff för de grova brotten. [24]
- Nya ungdomspåföljder. [25]
- En anpassning till dataskyddsförordningen – kreditupplysningslagen och några andra författningar. [26]
- Genomförande av säsongsanställningsdirektivet. [27]
- En snabbare lagföring. Försöksprojekt med ett snabbförfarande i brottmål. [36]
- Frekventa och omfattande ärenden om utlämnande av allmän handling. [37]
- Livstidsstraff för mord. [38]
- En omarbetad domstolsdatalog. Anpassning till EU:s dataskyddsförordning. [41]
- Följdändringar till ny förvaltningslag. [42]
- En omarbetad utlänningsdatalog. Anpassning till EU:s dataskyddsförordning. [45]

### Kulturdepartementet

- Kultursamverkan för ett Sverige som håller ihop. Framtida inriktning och utvecklingsmöjligheter för kultursamverkansmodellen. [8]
- Ändringar i bestämmelser om val till Sametinget. [34]
- Konsultation i frågor som rör det samiska folket. [43]

### Miljö- och energidepartementet

- Biologisk mångfald och ekosystemtjänster. Kontrollstation 2016. [32]
- Elmarknadslag. [44]

### **Näringsdepartementet**

- Effektivare sanktioner i livsmedelskedjan m.m. [5]
- En anpassning till dataskyddsförordningen av dataskyddsbestämmelser inom Näringsdepartementets verksamhetsområde. [28]

### **Socialdepartementet**

- Åldersdifferentierat underhållsstöd och höjt grundavdrag för bidragskyldiga föräldrar. [2]
- Sjukpenning i avvaktan på slutligt beslut. [4]
- Förslag till lag om ersättning till personer som har fått ändrad könstillhörighet fastställd i vissa fall. [6]
- Förstärkt rehabilitering för återgång i arbete. [9]
- Ändrade regler om retroaktivitet avseende efterlevandestöd. [11]
- Om förenklat beslutsfattande och särskilda boendeformer för äldre. [12]
- Vissa ändringar i läkemedelslagen. [14]
- Karensavdrag – en mer rättvis självrisk. [18]
- Utökade möjligheter till utbyte av läkemedel. [29]
- Legitimation för hälso- och sjukvårdskuratorer. [39]

### **Utrikesdepartementet**

- Ökat konsulärt skydd för unionsmedborgare och deras familjemedlemmar. Genomförande av direktiv (EU) 2015/637. [15]