Finansdepartementet

Finansmarknadsavdelningen

Författningsändringar på finansmarknadsområdet med anledning av EU:s dataskyddsförordning

Fi2017/03612/FPM

September 2017

Innehåll

1 Promemorians huvudsakliga innehåll

I april 2016 antogs EU:s allmänna dataskyddsförordning (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]). Genom förordningen införs enhetliga, generella krav på dataskyddshantering när det gäller personuppgifter. Förordningen ersätter dataskyddsdirektivet, som i svensk rätt har genomförts huvudsakligen genom personuppgiftslagen (1998:204), nedan förkortad PUL.

I denna promemoria övervägs och föreslås författningsändringar på finansmarknadsområdet i anledning av dataskyddsförordningen. Förslagen rör framför allt hänvisningar till PUL, vilka föreslås ska tas bort och i vissa fall ersättas av hänvisningar till dataskyddsförordningen.

Författningsändringarna föreslås träda i kraft den 25 maj 2018, vilket är samma dag som dataskyddsförordningen ska börja tillämpas.

2 Författningsförslag

2.1 Förslag till lag om ändring i lagen (1991:980) om handel med finansiella instrument

Härigenom föreskrivs att 2 kap. 12 § lagen (1991:980) om handel med finansiella instrument[1] ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	2 kap.
	12 §[2]
Inför upprättandet av ett prospekt och vid offentliggörande av det enligt 28–30 §§ får, i syfte att upprätta och offentliggöra prospektet *och utan hinder av 21 § personuppgiftslagen (1998:204)*, de personuppgifter behandlas som prospektet *skall* innehålla. I den utsträckning det krävs enligt 28–30 §§ får personuppgifterna i prospektet föras över till en stat utanför EES.	Inför upprättandet av ett prospekt och vid offentliggörande av det enligt 28–30 §§ får, i syfte att upprätta och offentliggöra prospektet, de personuppgifter behandlas som prospektet *ska* innehålla, *inklusive sådana uppgifter som avses i artikel 10 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv*

[1] Lagen omtryckt 1992:558.
[2] Senaste lydelse 2005:833.

95/46/EG (allmän dataskyddsförordning). I den utsträckning det krävs enligt 28–30 §§ får personuppgifterna i prospektet föras över till en stat utanför EES.

Denna lag träder i kraft den 25 maj 2018.

2.2 Förslag till lag om ändring i lagen (1998:1479) om värdepapperscentraler och kontoföring av finansiella instrument

Härigenom föreskrivs att 1 kap. 6 §, 4 kap. 1 § och 7 kap. 2 § lagen (1998:1479) om värdepapperscentraler och kontoföring av finansiella instrument[1] ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
6 §[2]	
Svenska värdepapperscentraler och kontoförande institut ska tillhandahålla ändamålsenliga rapporteringssystem för anställda som vill göra anmälningar om misstänkta överträdelser av de bestämmelser som gäller för verksamheten.	
Personuppgiftslagen (1998:204) gäller vid behandling av personuppgifter inom ramen för sådana rapporteringssystem som avses i första stycket.	
4 kap.	
1 §[3]	
Avstämningsregister består av avstämningskonton som läggs upp för ägare av finansiella instrument som registreras enligt denna lag. Sådana register förs med hjälp av automatiserad behandling. En svensk värdepapperscentral är personuppgiftsansvarig *enligt personuppgiftslagen (1998:204)* för den behandling av personuppgifter	Avstämningsregister består av avstämningskonton som läggs upp för ägare av finansiella instrument som registreras enligt denna lag. Sådana register förs med hjälp av automatiserad behandling. En svensk värdepapperscentral är personuppgiftsansvarig för den behandling av personuppgifter som den värdepapperscentralen utför.

[1] Senaste lydelse av lagens rubrik 2016:51.
[2] Senaste lydelse 2016:51. Ändringen innebär att andra stycket tas bort.
[3] Senaste lydelse 2016:51. Ändringen innebär bl.a. att andra stycket tas bort.

som den värdepapperscentralen utför.

Om inget annat följer av denna lag, av föreskrifter som meddelats med stöd av lagen, av förordningen om värdepapperscentraler eller av rättsakter som har antagits med stöd av förordningen, tillämpas personuppgiftslagen vid behandling av personuppgifter om ägare och innehavare av särskild rätt till finansiella instrument.

7 kap.

2 §[4]

För skada som tillfogas en ägare av ett finansiellt instrument till följd av en oriktig eller missvisande uppgift i ett avstämningsregister eller i annat fall genom fel i samband med upplägggning eller förande av ett sådant register svarar värdepapperscentralen eller, om felet kan hänföras till ett kontoförande institut, institutet. Ersättningsansvar gäller dock inte om värdepapperscentralen respektive det kontoförande institutet visar att felet beror på en omständighet utanför dess kontroll vars följder inte skäligen kunde ha undvikits eller övervunnits. Indirekt förlust ersätts endast om den beror på försummelse av värdepapperscentralen eller det kontoförande institutet. Detsamma gäller skada som tillfogas panthavare och den till vars förmån en rådighetsinskränkning gäller.

Ersättningsansvaret gäller på motsvarande sätt om felet beror på någon som har anlitats av värdepapperscentralen eller av ett kontoförande institut.

För skada som kan hänföras till ett kontoförande institut svarar värdepapperscentralen solidariskt med institutet. Värdepapperscentralens ansvar är dock i sådant fall begränsat till fem miljoner kronor för varje skadefall. Värdepapperscentralen har rätt till ersättning av det kontoförande institutet för vad

[4] Senaste lydelse 2016:51. Ändringen innebär att fjärde stycket tas bort.

värdepapperscentralen har betalat till följd av det solidariska ansvaret.

Bestämmelserna i personuppgiftslagen (1998:204) om skadestånd ska gälla då personuppgifter behandlats i strid med den lagen.

Denna lag träder i kraft den 25 maj 2018.

2.3 Förslag till lag om ändring i lagen (1999:889) om registrering av krigsskada på egendom

Härigenom föreskrivs att 1 § lagen (1999:889) om registrering av krigsskada på egendom ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 §
För det ändamål som anges i 3 § *skall* det föras ett för hela landet gemensamt register (krigsskaderegistret). Registret får föras med hjälp av automatisk databehandling.	För det ändamål som anges i 3 § *ska* det föras ett för hela landet gemensamt register (krigsskaderegistret). Registret får föras med hjälp av automatisk databehandling.
Ärenden om registrering *skall* handläggas av Finansinspektionen, som också är personuppgiftsansvarig *enligt personuppgiftslagen (1998:204)*.	Ärenden om registrering *ska* handläggas av Finansinspektionen, som också är personuppgiftsansvarig.
Närmare föreskrifter om vilka uppgifter registret *skall* innehålla meddelas av regeringen.	Närmare föreskrifter om vilka uppgifter registret *ska* innehålla meddelas av regeringen.

Denna lag träder i kraft den 25 maj 2018.

2.4 Förslag till lag om ändring i lagen (2004:46) om värdepappersfonder

Härigenom föreskrivs att 2 kap. 17 d § och 4 kap. 11 § lagen (2004:46) om värdepappersfonder[1] ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 kap.	
17 d §[2]	
Ett fondbolag ska tillhandahålla ändamålsenliga rapporteringssystem för anställda som vill göra anmälningar om misstänkta överträdelser av bestämmelser som gäller för verksamheten.	
Personuppgiftslagen (1998:204) gäller vid behandling av personuppgifter inom ramen för sådana rapporteringssystem som avses i första stycket.	
4 kap.	
11 §[3]	
Fondbolaget ska föra eller låta föra ett register över samtliga innehavare av andelar i fonden. *I fråga om automatiserad och viss manuell behandling av personuppgifter finns bestämmelser i personuppgiftslagen (1998:204).*	Fondbolaget ska föra eller låta föra ett register över samtliga innehavare av andelar i fonden.

Är lagen (1998:1479) om värdepapperscentraler och kontoföring av finansiella instrument tillämplig på andelarna i fonden, förs registret av en svensk värdepapperscentral. Fondbolaget har rätt till insyn i registret.

Om lagen om värdepapperscentraler och kontoföring av finansiella instrument inte är tillämplig på andelarna i fonden, ska den som för registret anteckna inskränkningar enligt

[1] Senaste lydelse av lagens rubrik 2013:563.
[2] Senaste lydelse 2016:892. Ändringen innebär att andra stycket tas bort.
[3] Senaste lydelse 2016:58.

13 kap. 19 § första stycket 4 eller 14 kap. 21 § första stycket 4 föräldrabalken där.

Fondbolaget ska till varje fondandelsägare skriftligen bekräfta att dennes fondandelsinnehav har registrerats. Av bekräftelsen ska det framgå värdepappersfondens och, i förekommande fall, andelsklassens beteckning samt namnen på fondbolaget och förvaringsinstitutet. Vidare ska det framgå var informationsbroschyren enligt 15 §, faktabladet enligt 16 a § samt årsberättelsen och halvårsredogörelsen enligt 18 § finns att tillgå.

Denna lag träder i kraft den 25 maj 2018.

2.5 Förslag till lag om ändring i lagen (2004:297) om bank- och finansieringsrörelse

Härigenom föreskrivs att 6 kap. 2 a § lagen (2004:297) om bank- och finansieringsrörelse ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	6 kap.
	2 a §[1]
	Ett kreditinstitut ska tillhandahålla ändamålsenliga rapporteringssystem för anställda som vill göra anmälningar om misstänkta överträdelser av bestämmelser som gäller för kreditinstitutets verksamhet.
	Personuppgiftslagen (1998:204) gäller vid behandling av personuppgifter inom ramen för sådana rapporteringssystem som avses i första stycket.

Denna lag träder i kraft den 25 maj 2018.

[1] Senaste lydelse 2014:982. Ändringen innebär att andra stycket tas bort.

2.6 Förslag till lag om ändring i lagen (2007:528) om värdepappersmarknaden

Härigenom föreskrivs att 4 kap. 8 §, 8 kap. 4 a §, 10 kap. 15 § och 13 kap. 2 a § lagen (2007:528) om värdepappersmarknaden ska ha följande lydelse.

Lydelse enligt SFS 2017:679	*Föreslagen lydelse*
4 kap.	
8 §[1]	
Ett företag som avses i 4 § och som har fått tillstånd att driva värdepappersrörelse från filial i Sverige ska tillhandahålla ändamålsenliga rapporteringssystem för anställda som vill göra anmälningar om misstänkta överträdelser av bestämmelser som gäller för verksamheten.	
Personuppgiftslagen (1998:204) gäller vid behandling av personuppgifter inom ramen för sådana rapporteringssystem.	

Nuvarande lydelse	*Föreslagen lydelse*
8 kap.	
4 a §[2]	
Ett värdepappersbolag ska tillhandahålla ändamålsenliga rapporteringssystem för anställda som vill göra anmälningar om misstänkta överträdelser av bestämmelser som gäller för verksamheten.	
Personuppgiftslagen (1998:204) gäller vid behandling av personuppgifter inom ramen för sådana rapporteringssystem som avses i första stycket.	

[1] Ändringen innebär att andra stycket tas bort.
[2] Senaste lydelse 2014:985. Ändringen innebär att andra stycket tas bort.

Lydelse enligt SFS 2017:679	*Föreslagen lydelse*

10 kap.

15 §[3]

Den som tillhandahåller en datarapporteringstjänst ska ha ändamålsenliga rapporteringssystem för anställda som vill göra anmälningar om misstänkta överträdelser av bestämmelser som gäller för verksamheten.

Personuppgiftslagen (1998:204) gäller vid behandling av personuppgifter inom ramen för sådana rapporteringssystem.

13 kap.

2 a §[4]

En börs ska tillhandahålla ändamålsenliga rapporteringssystem för anställda som vill göra anmälningar om misstänkta överträdelser av bestämmelser som gäller för verksamheten.

Personuppgiftslagen (1998:204) gäller vid behandling av personuppgifter inom ramen för sådana rapporteringssystem.

Denna lag träder i kraft den 25 maj 2018.

[3] Senaste lydelse 2017:679. Ändringen innebär att andra stycket tas bort.
[4] Senaste lydelse 2017:679. Ändringen innebär att andra stycket tas bort.

2.7 Förslag till lag om ändring i lagen (2010:751) om betaltjänster

Härigenom föreskrivs i fråga om lagen (2010:751) om betaltjänster

dels att 6 kap. 8 § ska upphöra att gälla,

dels att rubriken närmast före 6 kap. 8 § ska utgå,

dels att 6 kap. 1 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	6 kap.
	1 §
Om en betaltjänstleverantör eller den som ansvarar för ett betalningssystem granskar betalningstransaktioner för att kunna upptäcka sådana transaktioner som leverantören eller den ansvarige för betalningssystemet misstänker eller har skälig grund att misstänka utgör ett led i bedrägeri i samband med tillhandahållande eller användning av betaltjänster, får leverantören eller den som ansvarar för ett betalningssystem behandla personuppgifter samt föra register enligt 2–9 §§ *vilka gäller utöver personuppgiftslagen (1998:204)*.	Om en betaltjänstleverantör eller den som ansvarar för ett betalningssystem granskar betalningstransaktioner för att kunna upptäcka sådana transaktioner som leverantören eller den ansvarige för betalningssystemet misstänker eller har skälig grund att misstänka utgör ett led i bedrägeri i samband med tillhandahållande eller användning av betaltjänster, får leverantören eller den som ansvarar för ett betalningssystem behandla personuppgifter samt föra register enligt 2–9 §§.

Denna lag träder i kraft den 25 maj 2018.

2.8 Förslag till lag om ändring i försäkringsrörelselagen (2010:2043)

Härigenom föreskrivs att 4 kap. 14 § försäkringsrörelselagen (2010:2043) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
4 kap. 14 §	
En personuppgift som anger att en försäkringstagare har vidtagit dispositioner beträffande försäkringsbelopp som utfaller i framtiden till förmån för någon annan och som behandlas enligt *personuppgiftslagen (1998:204)* får inte lämnas ut till förmånstagaren.	En personuppgift som anger att en försäkringstagare har vidtagit dispositioner beträffande försäkringsbelopp som utfaller i framtiden till förmån för någon annan och som behandlas enligt *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)* får inte lämnas ut till förmånstagaren.

Denna lag träder i kraft den 25 maj 2018.

2.9 Förslag till lag om ändring i lagen om (2016:1306) med kompletterande bestämmelser till EU:s marknadsmissbruksförordning

Härigenom föreskrivs att 2 kap. 3 och 7 §§ lagen (2016:1306) med kompletterande bestämmelser till EU:s marknadsmissbruksförordning ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 kap.	
3 §	
Finansinspektionen ska föra eller låta föra register (insynsregister) över anmälningar som har gjorts enligt artikel 19.1–19.10 i marknadsmissbruksförordningen.	
Uppgifter som har lämnats av personer som inte längre omfattas av anmälningsskyldighet får tas bort ur registret.	
Registret ska föras med hjälp av automatisk databehandling. Finansinspektionen är personuppgiftsansvarig *enligt personuppgiftslagen (1998:204)* för den behandling av personuppgifter som sker i registret. Inspektionen ska på lämpligt sätt underrätta de registrerade om registret.	Registret ska föras med hjälp av automatisk databehandling. Finansinspektionen är personuppgiftsansvarig för den behandling av personuppgifter som sker i registret. Inspektionen ska på lämpligt sätt underrätta de registrerade om registret.
Registret ska vara offentligt.	
7 §	
Ett finansiellt företag ska tillhandahålla ändamålsenliga rapporteringssystem för anställda som vill göra anmälningar om misstänkta överträdelser av marknadsmissbruksförordningen.	
Personuppgiftslagen (1998:204) gäller vid behandling av personuppgifter inom ramen för sådana rapporteringssystem. Uppgifter om	*Personuppgifter* om lagöverträdelser som avses i *artikel 10 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016*

lagöverträdelser som avses i *21 § personuppgiftslagen* får *dock* behandlas om uppgifterna avser brott enligt lagen (2016:1307) om straff för marknadsmissbruk på värdepappersmarknaden.	*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)* får behandlas om uppgifterna avser brott enligt lagen (2016:1307) om straff för marknadsmissbruk på värdepappersmarknaden.

Denna lag träder i kraft den 25 maj 2018.

2.10 Förslag till lag om ändring i lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism

Härigenom föreskrivs i fråga om lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism

dels att 5 kap. 10 § ska upphöra att gälla,

dels att rubriken närmast före 5 kap. 10 § ska utgå,

dels att 5 kap. 1, 5 och 6 §§ och 6 kap. 4 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
5 kap.	
1 §[1]	
Detta kapitel gäller vid en verksamhetsutövares behandling av personuppgifter enligt denna lag. Kapitlet gäller om behandlingen helt eller delvis är 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.	
Personuppgiftslagen (1998:204) gäller vid verksamhetsutövarens behandling av personuppgifter, om inte annat följer av detta kapitel.	
5 §	
Känsliga personuppgifter som avses i *13 § personuppgiftslagen (1998:204)* får behandlas endast om det är nödvändigt för att	*Sådana särskilda kategorier av* personuppgifter som avses i *artikel 9.1 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om*

[1] Ändringen innebär att andra stycket tas bort.

upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) får behandlas endast om det är nödvändigt för att

1. bedöma om kunden är en person i politiskt utsatt ställning eller familjemedlem eller känd medarbetare till en sådan person enligt 1 kap. 8–10 §§,
2. bedöma den risk som kan förknippas med kundrelationen enligt 2 kap. 3 §,
3. uppfylla övervakningsskyldigheten enligt 4 kap. 1 §,
4. bedöma misstänkta transaktioner och aktiviteter enligt 4 kap. 2 §, och
5. lämna uppgifter enligt 4 kap. 3 och 6 §§.

Känsliga personuppgifter får också behandlas vid bevarande av handlingar och uppgifter enligt 3 och 4 §§, om det är tillåtet att behandla uppgifterna enligt första stycket.

6 §

Personuppgifter om lagöverträdelser som avses i *21 § personuppgiftslagen (1998:204)* får behandlas endast om det är nödvändigt för att

Personuppgifter om lagöverträdelser som avses i *artikel 10 i Europaparlamentets och rådets förordning (EU) 2016/679* får behandlas endast om det är nödvändigt för att

1. bedöma den risk som kan förknippas med kundrelationen enligt 2 kap. 3 §,
2. uppfylla övervakningsskyldigheten enligt 4 kap. 1 §,
3. bedöma misstänkta transaktioner och aktiviteter enligt 4 kap. 2 §, och
4. lämna uppgifter enligt 4 kap. 3 och 6 §§.

Uppgifter om lagöverträdelser får också behandlas vid bevarande av handlingar och uppgifter enligt 3 och 4 §§, om det är tillåtet att behandla uppgifterna enligt första stycket.

6 kap.

4 §[2]

En verksamhetsutövare ska tillhandahålla ändamålsenliga rapporteringssystem för anställda och uppdragstagare som vill

[2]Ändringen innebär att tredje stycket tas bort.

göra anmälningar om misstänkta överträdelser av bestämmelserna i denna lag eller föreskrifter som meddelats med stöd av lagen.

För verksamhetsutövare som omfattas av förordning (EU) 2015/847 ska rapporteringssystemen även möjliggöra anmälningar av misstänkta överträdelser av bestämmelserna i den förordningen.

Personuppgiftslagen (1998:204) gäller vid behandling av personuppgifter inom ramen för sådana rapporteringssystem som avses i första och andra styckena.

Denna lag träder i kraft den 25 maj 2018.

2.11 Förslag till lag om ändring i lagen (2017:631) om registrering av verkliga huvudmän

Härigenom föreskrivs att 2 kap. 6 § lagen (2017:631) om registrering av verkliga huvudmän ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 kap.	
6 §	
En juridisk person som avses i 4 eller 5 § och som har ett politiskt, religiöst, kulturellt eller annat sådant ändamål eller är ett trossamfund som inte registrerats i handelsregistret enligt handelsregisterlagen (1974:157) är inte skyldig att i anmälan ange uppgifter om fysiska personer som är medlemmar i den juridiska personen, om en sådan anmälan medför att medlemmens åskådning i något av dessa avseenden blir känd.	
Undantaget i första stycket gäller också om en anmälan *medför att en fysisk persons medlemskap i en fackförening blir känt eller om en anmälan avslöjar uppgift om en fysisk persons hälsotillstånd eller sexualliv*.	Undantaget i första stycket gäller också om en anmälan *annars avslöjar sådana särskilda kategorier av personuppgifter som avses i artikel 9.1 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)*.

Denna lag träder i kraft den 25 maj 2018.

2.12 Förslag till förordning om ändring i förordningen (2004:330) om inlåningsverksamhet

Härigenom föreskrivs i fråga om förordningen (2004:330) om inlåningsverksamhet

dels att 8 och 9 §§ ska upphöra att gälla,

dels att 6 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	6 §
Finansinspektionen är personuppgiftsansvarig *enligt personuppgiftslagen (1998:204)* för registret över företag som driver inlåningsverksamhet.	Finansinspektionen är personuppgiftsansvarig för registret över företag som driver inlåningsverksamhet.

Denna förordning träder i kraft den 25 maj 2018.

2.13 Förslag till förordning om ändring i förordningen (2004:329) om bank- och finansieringsrörelse

Härigenom föreskrivs i fråga om förordningen (2004:329) om bank- och finansieringsrörelse

dels att 4 kap. 7 och 9 §§ ska upphöra att gälla,

dels att 4 kap. 3, 4, 8 och 8 a §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
4 kap.	
3 §	
Bankregistret *skall* ge offentlighet åt den information som ingår i registret.	Bankregistret *ska* ge offentlighet åt den information som ingår i registret.
I fråga om personuppgifter *skall* registret ha till ändamål att tillhandahålla uppgifter för	I fråga om personuppgifter *ska* registret ha till ändamål att tillhandahålla uppgifter för
1. den tillsyn som Finansinspektionen har över banker enligt lagen (2004:297) om bank- och finansieringsrörelse,	
2. affärsverksamhet, kreditgivning eller någon annan allmän eller enskild verksamhet där företagsanknuten information utgör underlag för prövningar eller beslut,	
3. förvärv, avyttring eller förvaltning av banker som registreras i bankregistret,	
4. aktualisering, komplettering eller kontroll av företagsanknuten information som finns i kund- eller medlemsregister eller liknande register,	
5. uttag av urval av personuppgifter för direkt marknadsföring, dock med den begränsning som följer av *11 § personuppgiftslagen (1998:204)*, eller	5. uttag av urval av personuppgifter för direkt marknadsföring, dock med den begränsning som följer av *artikel 21.2 och 21.3 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om*

	upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), eller

6. verksamhet för vilken staten eller en kommun ansvarar enligt lag eller annan författning och

a) som avser banker som registreras i bankregistret,

b) som för att kunna utföras förutsätter tillgång till företagsanknuten information, eller

c) som avser fullgörande av underrättelseskyldighet.

4 §	
Bolagsverket är personuppgiftsansvarig *enligt personuppgiftslagen (1998:204)* för bankregistret.	Bolagsverket är personuppgiftsansvarig för bankregistret.
8 §	
I fråga om rättelse av personuppgifter i bankregistret *skall* 26 § förvaltningslagen (1986:223) tillämpas i stället för *28 § personuppgiftslagen (1998:204)*.	I fråga om rättelse av personuppgifter i bankregistret *ska* 26 § förvaltningslagen (1986:223) tillämpas i stället för *artikel 16 i Europaparlamentets och rådets förordning (EU) 2016/679*.
8 a §[1]	
Information som ska lämnas enligt *26 § personuppgiftslagen (1998:204)* behöver inte omfatta uppgift i en handling som har kommit in till Bolagsverket, om den enskilde har tagit del av handlingens innehåll. Om den enskilde begär det, ska dock informationen även omfatta uppgift i en sådan handling.	Information som ska lämnas enligt *artikel 15 i Europaparlamentets och rådets förordning (EU) 2016/679* behöver inte omfatta uppgift i en handling som har kommit in till Bolagsverket, om den enskilde har tagit del av handlingens innehåll. Om den enskilde begär det, ska dock informationen även omfatta uppgift i en sådan handling.

[1] Senaste lydelse 2007:1468.

Om informationen inte innehåller en handling som avses i första stycket, ska det av informationen framgå att handlingen behandlas av myndigheten.

Denna förordning träder i kraft den 25 maj 2018.

2.14 Förslag till förordning om ändring i förordningen (2004:331) om valutaväxling och annan finansiell verksamhet

Härigenom föreskrivs i fråga om förordningen (2004:331) om valutaväxling och annan finansiell verksamhet[1]

dels att 7 och 8 §§ ska upphöra att gälla,

dels att 5 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	5 §[2]
Finansinspektionen är personuppgiftsansvarig *enligt personuppgiftslagen (1998:204)* för registret.	Finansinspektionen är personuppgiftsansvarig för registret.

Denna förordning träder i kraft den 25 maj 2018.

[1] Senaste lydelse av förordningens rubrik 2017:670.
[2] Senaste lydelse 2017:670.

2.15 Förslag till förordning om ändring i förordningen (2007:572) om värdepappersmarknaden

Härigenom föreskrivs i fråga om förordningen (2007:572) om värdepappersmarknaden

dels att 3 kap. 10 § ska upphöra att gälla,

dels att 3 kap. 6 och 11 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
3 kap.	
6 §	
Registrering av anknutna ombud görs i registret över anknutna ombud. Registret förs med hjälp av automatiserad behandling och *skall* hållas tillgängligt hos Bolagsverket. Verket är personuppgiftsansvarigt *enligt personuppgiftslagen (1998:204)* för registret.	Registrering av anknutna ombud görs i registret över anknutna ombud. Registret förs med hjälp av automatiserad behandling och *ska* hållas tillgängligt hos Bolagsverket. Verket är personuppgiftsansvarigt för registret.
I registret över anknutna ombud registreras uppgifter för varje anknutet ombud.	
11 §	
I fråga om rättelse av personuppgifter i registret över anknutna ombud *skall* 26 § förvaltningslagen (1986:223) tillämpas i stället för *28 § personuppgiftslagen (1998:204)*.	I fråga om rättelse av personuppgifter i registret över anknutna ombud *ska* 26 § förvaltningslagen (1986:223) tillämpas i stället för *artikel 16 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv*

95/46/EG (allmän dataskyddsförordning).

Denna förordning träder i kraft den 25 maj 2018.

2.16 Förslag till förordning om ändring i förordningen (2009:92) om åtgärder mot penningtvätt och finansiering av terrorism

Härigenom föreskrivs i fråga om förordningen (2009:92) om åtgärder mot penningtvätt och finansiering av terrorism

dels att 10 § ska upphöra att gälla,

dels att 5 och 11 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
5 §[1]	
Bolagsverket ska med hjälp av automatiserad databehandling föra ett register över de verksamhetsutövare som har gjort anmälan enligt 7 kap. 3 § lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism.	
Bolagsverket är personuppgiftsansvarigt för registret *enligt personuppgiftslagen (1998:204)*.	Bolagsverket är personuppgiftsansvarigt för registret.
11 §	
I fråga om rättelse av personuppgifter i registret ska 26 § förvaltningslagen (1986:223) tillämpas i stället för *28 § personuppgiftslagen (1998:204)*.	I fråga om rättelse av personuppgifter i registret ska 26 § förvaltningslagen (1986:223) tillämpas i stället för *artikel 16 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv*

[1] Senaste lydelse 2017:675.

95/46/EG (allmän dataskyddsförordning).

Denna förordning träder i kraft den 25 maj 2018.

2.17 Förslag till förordning om ändring i förordningen (2010:1008) om betaltjänster

Härigenom föreskrivs i fråga om förordningen (2010:1008) om betaltjänster

dels att 2 § ska upphöra att gälla,

dels att 1 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 §
Finansinspektionen är personuppgiftsansvarig *enligt personuppgiftslagen (1998:204)* för det register som förs enligt 8 kap. 5 § lagen (2010:751) om betaltjänster.	Finansinspektionen är personuppgiftsansvarig för det register som förs enligt 8 kap. 5 § lagen (2010:751) om betaltjänster.

Denna förordning träder i kraft den 25 maj 2018.

2.18 Förslag till förordning om ändring i försäkringsrörelseförordningen (2011:257)

Härigenom föreskrivs i fråga om försäkringsrörelseförordningen (2011:257)

dels att 4 kap. 10, 12 och 13 §§ ska upphöra att gälla,

dels att rubrikerna närmast före 4 kap. 10 och 12 §§ ska utgå,

dels att 4 kap. 5, 7 och 11 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
4 kap.	
5 §	
Försäkringsregistret ska ge offentlighet åt den information som ingår i registret.	
I fråga om personuppgifter ska registret ha till ändamål att tillhandahålla uppgifter för	
1. den tillsyn som Finansinspektionen har över försäkringsföretagen enligt försäkringsrörelselagen (2010:203),	
2. affärsverksamhet, kreditgivning eller annan allmän eller enskild verksamhet där företagsanknuten information utgör underlag för prövningar eller beslut,	
3. förvärv, avyttring eller förvaltning av försäkringsföretag som registreras i försäkringsregistret,	
4. aktualisering, komplettering eller kontroll av företagsanknuten information som finns i kund- eller medlemsregister eller liknande register,	
5. uttag av urval av personuppgifter för direkt marknadsföring, dock med den begränsning som följer av *11 § personuppgiftslagen (1998:204)*, eller	5. uttag av urval av personuppgifter för direkt marknadsföring, dock med den begränsning som följer av *artikel 21.2 och 21.3 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv*

95/46/EG (allmän dataskyddsförordning), eller

6. verksamhet som staten eller en kommun ansvarar för enligt lag eller annan författning, och

a) som avser försäkringsföretag som registreras i försäkringsregistret,

b) som för att kunna utföras förutsätter tillgång till företagsanknuten information, eller

c) som avser fullgörande av underrättelseskyldighet.

7 §

Bolagsverket är personuppgiftsansvarigt *enligt personuppgiftslagen (1998:204)* för försäkringsregistret.

Bolagsverket är personuppgiftsansvarigt för försäkringsregistret.

11 §

I fråga om rättelse av personuppgifter i försäkringsregistret tillämpas 26 § förvaltningslagen (1986:223) i stället för *28 § personuppgiftslagen (1998:204)*.

I fråga om rättelse av personuppgifter i försäkringsregistret tillämpas 26 § förvaltningslagen (1986:223) i stället för *artikel 16 i Europaparlamentets och rådets förordning (EU) 2016/679*.

Denna förordning träder i kraft den 25 maj 2018.

2.19 Förslag till förordning om ändring i förordningen (2011:776) om elektroniska pengar

Härigenom föreskrivs i fråga om förordningen (2011:776) om elektroniska pengar

dels att 3 § ska upphöra att gälla,

dels att 2 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	2 §
Finansinspektionen är personuppgiftsansvarig *enligt personuppgiftslagen (1998:204)* för det register som förs enligt 5 kap. 5 § lagen (2011:755) om elektroniska pengar.	Finansinspektionen är personuppgiftsansvarig för det register som förs enligt 5 kap. 5 § lagen (2011:755) om elektroniska pengar.

Denna förordning träder i kraft den 25 maj 2018.

2.20 Förslag till förordning om ändring i förordningen (2014:397) om viss verksamhet med konsumentkrediter

Härigenom föreskrivs i fråga om förordningen (2014:397) om viss verksamhet med konsumentkrediter

dels att 2 § ska upphöra att gälla,

dels att 1 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 §
Finansinspektionen är personuppgiftsansvarig *enligt personuppgiftslagen (1998:204)* för det register som förs enligt 15 § lagen (2014:275) om viss verksamhet med konsument-krediter.	Finansinspektionen är personuppgiftsansvarig för det register som förs enligt 15 § lagen (2014:275) om viss verksamhet med konsument-krediter.

Denna förordning träder i kraft den 25 maj 2018.

2.21 Förslag till förordning om ändring i förordningen (2016:1033) om verksamhet med bostadskrediter

Härigenom föreskrivs i fråga om förordningen (2016:1033) om verksamhet med bostadskrediter

dels att 5 § ska upphöra att gälla,

dels att 3 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	3 §
Finansinspektionen är personuppgiftsansvarig *enligt personuppgiftslagen (1998:204)* för det register som förs enligt 5 kap. 1 § lagen (2016:1024) om verksamhet med bostadskrediter.	Finansinspektionen är personuppgiftsansvarig för det register som förs enligt 5 kap. 1 § lagen (2016:1024) om verksamhet med bostadskrediter.

Denna förordning träder i kraft den 25 maj 2018.

2.22 Förslag till förordning om ändring i förordningen (2016:1316) med kompletterande bestämmelser till EU:s marknadsmissbruksförordning

Härigenom föreskrivs i fråga om förordningen (2016:1316) med kompletterande bestämmelser till EU:s marknadsmissbruksförordning

dels att 6 § ska upphöra att gälla,

dels att rubriken närmast före 6 § ska utgå,

dels att 3 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	3 §
Finansinspektionen får i utredningssyfte föra ett register (utredningsregistret) i ärenden som rör överträdelse som kan föranleda sanktion enligt 5 kap. 1 § lagen (2016:1306) med kompletterande bestämmelser till EU:s marknadsmissbruksförordning.	
Registret får föras med hjälp av automatiserad behandling. Inspektionen är personuppgiftsansvarig *enligt personuppgiftslagen (1998:204)* för den behandling av personuppgifter som sker i registret.	Registret får föras med hjälp av automatiserad behandling. Inspektionen är personuppgiftsansvarig för den behandling av personuppgifter som sker i registret.
Utredningsregistret får endast innehålla uppgifter som	
1. hämtats in genom terminalåtkomst enligt 8 kap. 3 § andra stycket lagen (1998:1479) om värdepapperscentraler och kontoföring av finansiella instrument,	
2. lämnats ut av värdepapperscentral enligt 8 kap. 3 § första stycket samma lag,	
3. på begäran lämnats av någon enligt 3 kap. 1 § lagen med kompletterande bestämmelser till EU:s marknadsmissbruksförordning,	
4. lämnats av en utländsk tillsynsmyndighet,	
5. lämnats av annan myndighet, eller	
6. inhämtats i samband med en platsundersökning efter beslut i domstol enligt 4 kap. lagen med kompletterande bestämmelser till EU:s marknadsmissbruksförordning.	

Till registret får också uppgifter hämtas in från insynsregistret.

Denna förordning träder i kraft den 25 maj 2018.

2.23 Förslag till förordning om ändring i förordningen (2017:667) om registrering av verkliga huvudmän

Härigenom föreskrivs i fråga om förordningen (2017:667) om registrering av verkliga huvudmän

dels att 3 kap. 7 § ska upphöra att gälla,

dels att 3 kap. 1, 6, 8 och 9 §§ och 5 kap. 5 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
3 kap.	
1 §	
Registret över verkliga huvudmän förs med hjälp av automatiserad behandling. Registret ska hållas tillgängligt hos Bolagsverket.	
Bolagsverket är personuppgiftsansvarigt *enligt personuppgiftslagen (1998:204)* för registret över verkliga huvudmän.	Bolagsverket är personuppgiftsansvarigt för registret över verkliga huvudmän.
6 §	
Information som ska lämnas *enligt 26 § personuppgiftslagen (1998:204)* behöver inte omfatta uppgift i en handling som har kommit in till Bolagsverket, om den enskilde har tagit del av handlingens innehåll. Om den enskilde begär det, ska dock informationen även omfatta uppgift i en sådan handling.	Information som ska lämnas enligt *artikel 15 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)* behöver inte omfatta uppgift i en handling som har kommit in till Bolagsverket, om den enskilde

	har tagit del av handlingens innehåll. Om den enskilde begär det, ska dock informationen även omfatta uppgift i en sådan handling.

Om informationen inte innehåller en handling som avses i första stycket, ska det av informationen framgå att handlingen behandlas av myndigheten.

8 §

I fråga om rättelse av personuppgifter i registret ska 26 § förvaltningslagen (1986:223) tillämpas i stället för *28 § personuppgiftslagen (1998:204)*.	I fråga om rättelse av personuppgifter i registret ska 26 § förvaltningslagen (1986:223) tillämpas i stället för *artikel 16 i Europaparlamentets och rådets förordning (EU) 2016/679*.

9 §

Vid sökning i registret får uppgifter som *avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv* inte användas som sökbegrepp.	Vid sökning i registret får *sådana särskilda kategorier av* personuppgifter som *avses i artikel 9.1 i Europaparlamentets och rådets förordning (EU) 2016/679* inte användas som sökbegrepp.

5 kap.

5 §

I 22 a § förvaltningslagen (1986:223) finns bestämmelser om överklagande till allmän förvaltningsdomstol. Andra beslut *än beslut enligt 2 kap. 1 § andra stycket* får *dock* inte överklagas.	I 22 a § förvaltningslagen (1986:223) finns bestämmelser om överklagande till allmän förvaltningsdomstol. *Beslut enligt 2 kap. 1 § andra stycket och beslut som en myndighet fattar med anledning av att en registrerad utövar sina rättigheter enligt artiklarna 12.5, 15–19 eller 21 i Europaparlamentets och*

rådets förordning (EU) 2016/679 får överklagas. Andra beslut *enligt denna förordning* får inte överklagas.

Denna förordning träder i kraft den 25 maj 2018.

3 Dataskyddsreformen

3.1 Reformens syfte

Den allmänna regleringen för behandling av personuppgifter inom EU finns i dag i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om behandling av det fria flödet av sådana uppgifter (dataskyddsdirektivet). Direktivet syftar till att garantera en hög och i alla medlemsstater likvärdig skyddsnivå när det gäller enskilda personers fri- och rättigheter med avseende på behandling av personuppgifter, samt att främja ett fritt flöde av personuppgifter mellan medlemsstaterna i EU. Dataskyddsdirektivet gäller inte för behandling av personuppgifter på områden som faller utanför gemenskapsrätten, t.ex. allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område. Dataskyddsdirektivet har genomförts i svensk rätt genom PUL, som är generellt tillämplig vid behandling av personuppgifter. Därtill finns ett antal sektorspecifika författningar som reglerar behandling av personuppgifter hos framför allt myndigheter, s.k. registerförfattningar.

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

Den 27 april 2016 antogs 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). Dataskyddsförordningen utgör en ny generell reglering för personuppgiftsbehandling inom EU och kommer att ersätta det nuvarande dataskyddsdirektivet när den börjar tillämpas den 25 maj 2018.

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. Till skillnad från EU-direktiv ska alltså förordningar inte genomföras i nationell rätt. I stället ska bestämmelserna i en EU-förordning tillämpas av enskilda, myndigheter och domstolar precis som om de vore bestämmelser i nationella författningar. Även om dataskyddsförordningen är direkt tillämplig, till skillnad från dataskyddsdirektivet, innehåller den många bestämmelser som förutsätter eller ger utrymme för kompletterande nationella bestämmelser av olika slag.

Samtidigt med dataskyddsförordningen antogs ett nytt dataskyddsdirektiv med regler om behandling av personuppgifter inom den brottsbekämpande sektorn, 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 verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF. Sådan behandling som omfattas av det nya dataskyddsdirektivet är undantagen från dataskyddsförordningens tillämpningsområde.

Det huvudsakliga syftet med reformen är att ytterligare harmonisera och effektivisera skyddet för personuppgifter för att bl.a. förbättra den inre marknadens funktion och öka enskildas kontroll över sina personuppgifter.

3.2 Dataskyddsförordningen

Dataskyddsförordningen trädde i kraft den 24 maj 2016 och ska som nämns ovan tillämpas fr.o.m. den 25 maj 2018.

Dataskyddsförordningen kommer att utgöra den generella rättsliga grunden för personuppgiftsbehandling inom EU. I förordningens första kapitel slås syftet och tillämpningsområdet fast. Utgångspunkten är att förordningen ska tillämpas på all behandling av personuppgifter, om uppgifterna rör en fysisk

person och behandlingen helt eller delvis sker på automatisk väg eller avser personuppgifter som ingår i eller kommer att ingå i ett register. Från tillämpningsområdet undantas dock behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten och behandling som utförs av medlemsstaterna när de bedriver verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken. Vidare undantas behandling som utförs av en fysisk person som ett led i verksamhet av rent privat natur eller som har samband med dennes hushåll och behandling som utförs av EU:s institutioner, organ och byråer. Slutligen undantas behandling som utförs av behöriga myndigheter i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten (sådan behandling av personuppgifter omfattas i stället av ovan nämnda direktiv [EU] 2016/680).

I dataskyddsförordningen anges de principer som ska styra behandlingen av personuppgifter (kapitel 2), de rättigheter som den registrerade ska ha (kapitel 3), de skyldigheter som den personuppgiftsansvarige och dennes biträde, det s.k. personuppgiftsbiträdet, ska ha (kapitel 4) samt det som ska gälla vid överföring av personuppgifter till tredjeländer eller internationella organisationer (kapitel 5). I förordningen finns också bestämmelser om oberoende nationella tillsynsmyndigheter (kapitel 6) och deras samarbete och åtgärder som de ska vidta för att förordningen ska tillämpas konsekvent (kapitel 7). Vidare finns bestämmelser om rättsmedel, ansvar och sanktioner (kapitel 8) och delegerade befogenheter (kapitel 10).

Dataskyddsförordningen baseras till stor del på dataskyddsdirektivets struktur och innehåll men innehåller även nyheter. Till exempel ökar informationsskyldigheten till den registrerade och administrativa sanktionsavgifter införs. För att förordningen ska tillämpas konsekvent i hela EU, inrättas Europeiska dataskyddsstyrelsen, som kommer att bestå av representanter för de nationella dataskyddsmyndigheterna.

Förordningen är direkt tillämplig i medlemsstaterna men förutsätter och möjliggör kompletterande nationella bestämmelser. Medlemsstaterna ska t.ex., för behandling som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller

litterärt skapande, fastställa undantag eller avvikelser från vissa av förordningens bestämmelser, bl.a. rörande principer för personuppgiftsbehandling, om dessa är nödvändiga för att förena rätten till integritet med yttrande- och informationsfriheten (artikel 85.2). Vidare finns det ett förhållandevis stort utrymme för nationella särregleringar för sådan personuppgiftsbehandling som är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse eller utföra en uppgift av allmänt intresse eller som är nödvändig som ett led i den personuppgiftsansvariges myndighetsutövning (artikel 6.2).

3.3 Generella nationella bestämmelser som kompletterar dataskyddsförordningen

Regeringen tillsatte under våren 2016 en utredning med uppdraget att föreslå de anpassningar och kompletterande författningsändringar på generell nivå som dataskyddsförordningen ger anledning till (Dataskyddsutredningen). Dataskyddsutredningen lämnade den 12 maj 2017 sitt betänkande Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning (SOU 2017:39). I betänkandet föreslås bl.a. att PUL ska upphävas och att det ska införas en lag med kompletterande bestämmelser till EU:s dataskyddsförordning.

Dataskyddsutredningens förslag på nationell reglering omfattar bestämmelser som på ett generellt plan dels kompletterar, dels gör undantag från förordningen (Förslag till lag med kompletterande bestämmelser till EU:s dataskyddsförordning, förkortad dataskyddslagen). Dataskyddsutredningens arbete och betänkande omfattar emellertid inte en översyn eller förslag till ändringar av sådan sektorsspecifik reglering av behandling av personuppgifter som finns bl.a. i särskilda registerförfattningar för myndigheter eller i andra författningar som rör sektorspecifik behandling av personuppgifter. De av utredningens förslag som har särskild betydelse för denna promemoria berörs särskilt i relevanta avsnitt nedan.

Därutöver har Utredningen om tillsynen över den personliga integriteten lämnat förslag på anpassningar i anledning av dataskyddsreformens bestämmelser om tillsyn (SOU 2016:65).

Bland annat föreslås att Datainspektionen ska utses till svensk nationell tillsynsmyndighet enligt dataskyddsförordningen. Dataskyddsutredningen utgår från det förslaget i sitt betänkande (SOU 2017:39 s. 93).

4 Översynen i promemorian

4.1 Den sektorsspecifika dataskyddsregleringen

Som nämns ovan (avsnitt 3.3) har Dataskyddsutredningens uppdrag inte omfattat att se över eller lämna förslag till ändringar av sektorsspecifik reglering av behandling av personuppgifter med anledning av dataskyddsförordningen.

Den sammantagna svenska dataskyddsregleringen är omfattande. Till exempel finns ett flertal registerförfattningar, dvs. sektors- eller myndighetsspecifika författningar som innehåller bestämmelser om statliga och kommunala myndigheters behandling av personuppgifter. Dessa författningar kompletterar eller avviker från PUL, som är subsidiär (se 2 § PUL). Vissa registerförfattningar innehåller närmast heltäckande dataskyddsregler, medan andra registerförfattningar endast upplyser om t.ex. att PUL:s bestämmelser om skadestånd och rättelse gäller även för informationshantering enligt författningen i fråga. Utöver registerförfattningarna finns det författningar som innehåller bestämmelser om personuppgiftsbehandling men som helt saknar regler om registerföring. Vidare finns det författningar som innehåller enstaka bestämmelser om personuppgiftsbehandling, som riktar sig till enskilda aktörer.

På finansmarknadsområdet finns flera författningar med inslag av dataskyddsreglering. Dessa måste anpassas till dataskyddsförordningen och de ändringar av svensk rätt som förordningen medför (jfr avsnitt 4.2).

4.2 Dataskyddsregleringen på finansmarknadsområdet

Promemorians bedömning: De författningar på finansmarknadsområdet som innehåller inslag av dataskyddsreglering omfattas av dataskyddsförordningens tillämpningsområde.

Skälen för promemorians bedömning: Dataskyddsförordningens tillämpningsområde behandlas i avsnitt 3.2. För att de författningar på finansmarknadsområdet som innehåller inslag av dataskyddsreglering ska omfattas av förordningens tillämpningsområde är det avgörande om de avser en verksamhet som omfattas av unionsrätten (artikel 2.2 a i dataskyddsförordningen). Vilka verksamheter som omfattas av unionsrättens tillämpningsområde följer av fördragen och EU-domstolens praxis.

Författningarna på finansmarknadsområdet reglerar förhållanden som utgör en del av den inre marknaden och som omfattas av unionsrätten och omfattas därför av dataskyddsförordningens tillämpningsområde. De behöver därför ses över och vid behov anpassas till dataskyddsförordningen.

I sammanhanget kan nämnas att Dataskyddsutredningen föreslår att dataskyddsförordningen – och den föreslagna nya dataskyddslagen – även ska tillämpas vid behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten (1 kap. 2 § dataskyddslagen).

4.3 Utgångspunkter och tillvägagångssätt

Som framgår av avsnitt 3.3 lämnar Dataskyddsutredningen förslag på nationell reglering som dels upphäver PUL och personuppgiftsförordningen (1998:1191), förkortad PUF, dels på ett generellt plan kompletterar, och gör undantag från, dataskyddsförordningen. Dessa förslag har ännu inte lett till lagstiftning. Det finns emellertid i dagsläget inte anledning att anta annat än att den svenska generella dataskyddsregleringen i framtiden kommer att ha i allt väsentligt den utformning som utredningen föreslår. De förslag som lämnas i denna promemoria är därför utformade med utgångspunkt i Dataskyddsutredningens förslag.

Någon förteckning över samtliga författningar med inslag av dataskyddsreglering finns inte. För att identifiera de författningar på finansmarknadsområdet som berörs av dataskyddsreformen har dessa författningar därför gåtts igenom med fokus på dataskyddsinslag. Vidare har sökningar gjorts i rättsdatabaser. Den senare metoden är densamma som användes av Informationshanteringsutredningen (Ju 2011:11) vid den inventering som gjordes inom ramen för arbetet med betänkandet Myndighetsdatalag (SOU 2015:39).

Promemorian behandlar i några fall bestämmelser som rör personuppgiftsbehandling som införts genom ett annat lagstiftningsärende och som ännu inte har trätt i kraft (prop. 2016/17:162, bet. 2016/17:FiU35, rskr. 2016/17:353). Det handlar om nya bestämmelser i lagen (2007:528) om värdepappersmarknaden som träder i kraft den 3 januari 2018 (SFS 2017:679). Dessa bestämmelser kommer att ha trätt i kraft när dataskyddsförordningen ska börja tillämpas och de behandlas därför i promemorians lagförslag som gällande rätt vid den tidpunkt när lagförslagen i promemorian föreslås träda i kraft.

5 Krav på behandlingen av personuppgifter

5.1 Tillåten personuppgiftsbehandling

Promemorians bedömning: Sådan behandling av personuppgifter som är nödvändig till följd av författningar på finansmarknadsområdet kan ske med stöd av dataskyddsförordningen. Det finns därför inte något behov av författningsändringar i detta avseende.

Skälen för promemorians bedömning

Personuppgiftslagens krav

För att personuppgiftsbehandling ska vara tillåten ska, enligt 10 § PUL, den registrerade ha lämnat sitt samtycke till behandlingen eller behandlingen vara nödvändig för något av de i paragrafen angivna ändamålen. Därutöver finns i 9 § PUL vissa grundläggande krav på all behandling av personuppgifter. Den personuppgiftsansvarige ska bl.a. se till att personuppgifter behandlas lagligt och på ett korrekt sätt samt att personuppgifter bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Vidare får de insamlade uppgifterna inte användas på ett sätt som är oförenligt med det ändamål för vilket de samlades in (den s.k. finalitetsprincipen) eller bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Avser behandlingen s.k. känsliga personuppgifter eller uppgifter om lagöverträdelser m.m., måste behandlingen dessutom vara tillåten enligt 13–21 §§ PUL, vilket behandlas närmare i avsnitten 5.2 och 5.3.

Dataskyddsförordningens krav

De villkor som ska vara uppfyllda för att behandling av personuppgifter ska vara laglig anges i artikel 6 i dataskyddsförordningen. Artikelns innehåll överensstämmer i stort med 10 § PUL.

Av artikel 6.1 följer att behandlingen är laglig endast 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 vilar på 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 gäller dock inte för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter.

Medlemsstaterna får enligt artikel 6.2 i dataskyddsförordningen närmare fastställa specifika krav för uppgiftsbehandlingen och andra åtgärder för att säkerställa en laglig och rättvis behandling för att efterleva artikel 6.1 första stycket c och e.

Den grund för behandling som avses i artikel 6.1 första stycket c och e ska enligt artikel 6.3 fastställas i enlighet med unionsrätten eller den medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av. Också syftet med behandlingen ska fast-

ställas i den rättsliga grunden eller, i fråga om behandling enligt artikel 6.1 första stycket e, vara nödvändigt för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

Av artikel 6.3 följer vidare att den rättsliga grunden kan innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen, bl.a. de allmänna villkor som ska gälla, vilken typ av uppgifter som ska behandlas, ändamålsbegränsningar och lagringstid.

Artikel 6.3 ställer också krav på att, i fråga om grunden för personuppgiftsbehandling, unionsrätten eller medlemsstaternas nationella rätt ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas. Detta krav på proportionalitet, som gäller även för sektorsspecifika dataskyddsbestämmelser, torde enligt Dataskyddsutredningen innebära att lagstiftaren måste göra en avvägning mellan å ena sidan behovet av att en uppgift kan utföras på ett effektivt och rättssäkert sätt och, å andra sidan, den enskildes rätt till skydd för sina personuppgifter (SOU 2017:39 s. 134).

Slutligen berör artikel 6.4 situationen att en behandling sker för andra ändamål än det ändamål för vilket personuppgifterna ursprungligen samlades in.

Utöver kravet på rättslig grund i artikel 6 finns i artikel 5 i dataskyddsförordningen vissa grundläggande principer för personuppgiftsbehandling. Enligt den artikeln ska personuppgifter behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Vidare anges och utvecklas vissa principer som gäller vid personuppgiftsbehandling, nämligen principerna om ändamålsbegränsning, uppgiftsminimering, korrekthet, lagringsminimering samt integritet och konfidentialitet. Slutligen anges att det är den personuppgiftsansvarige som ansvarar för, och ska kunna visa, att de grundläggande principerna efterlevs. Skyldigheterna i bl.a. artikel 5 kan, under vissa förutsättningar, begränsas genom unionsrätten eller medlemsstaternas nationella rätt (artikel 23).

I likhet med PUL finns det i dataskyddsförordningen ytterligare krav för behandling av känsliga personuppgifter och för behandling av uppgifter som rör fällande domar i brottmål och överträdelser (artikel 9 respektive 10). Artiklarna 9 och 10 behandlas närmare i avsnitten 5.2 och 5.3.

Dataskyddsförordningens krav kan förenklat sammanfattas som att personuppgiftsbehandlingen måste ha en rättslig grund, dvs. antingen ske med samtycke (artikel 6.1 första stycket a) eller uppfylla villkoren i något av leden b–f i artikel 6.1 första stycket. Detta är emellertid inte tillräckligt för att en behandling av personuppgifter ska vara tillåten. Övriga krav måste också vara uppfyllda, t.ex. de grundläggande principerna för behandling i artikel 5. Behovet av den konkreta behandlingen måste alltid vägas mot den registrerades intresse av personlig integritet.

Dataskyddsutredningens förslag

Dataskyddsutredningen överväger frågan vad som avses med att grunden för personuppgiftsbehandlingen enligt artikel 6.1 första stycket c och e ska fastställas i enlighet med unionsrätten eller den medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av (artikel 6.3).

Enligt utredningens bedömning avses med ”grunden för behandlingen” den rättsliga förpliktelsen, uppgiften av allmänt intresse respektive myndighetsutövningen (jfr artikel 6.1 första stycket c och e), dvs. det är uppgiften/förpliktelsen/myndighetsutövningen som ska vara fastställd, inte själva behandlingen. Det innebär inte att det krävs en särskild reglering just med anledning av att dataskyddsförordningen ska börja tillämpas. Den rättsliga förpliktelsen, uppgiften av allmänt intresse eller myndighetsutövningen måste däremot vara rättsligt förankrad i unionsrätten eller nationell rätt för att kunna åberopas som rättslig grund för personuppgiftsbehandling. Det krävs inte att uppgiften, förpliktelsen eller myndighetsutövningen framgår av lag, men grunden ska vara fastställd i laga ordning, dvs. på ett konstitutionellt korrekt sätt. Dessutom ska den rättsliga grunden vara tydlig och precis och dess tillämpning förutsägbar (SOU 2017:39 s. 112).

Utredningen föreslår att det i lag ska anges att personuppgifter får behandlas med stöd av artikel 6.1 första stycket c i dataskyddsförordningen, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som gäller enligt lag eller annan författning eller som följer av kollektivavtal eller av beslut som har meddelats med stöd av lag

eller annan författning (2 kap. 3 § dataskyddslagen). Utredningen föreslår vidare att det på motsvarande sätt ska anges att personuppgifter får behandlas med stöd av artikel 6.1 första stycket e i dataskyddsförordningen om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna utföra en uppgift av allmänt intresse som följer av lag eller annan författning eller som följer av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning eller om behandlingen är nödvändig som ett led i myndighetsutövning som den personuppgiftsansvarige utövar enligt lag eller annan författning (2 kap. 4 § dataskyddslagen).

Det finns rättsligt stöd för nödvändig personuppgiftsbehandling på finansmarknadsområdet

På finansmarknadsområdet finns ett antal författningar i vilka såväl myndigheter som privata aktörer åläggs uppgifter och förpliktelser som kräver behandling av personuppgifter. Som exempel kan nämnas Bolagsverkets skyldighet enligt 4 kap. 1 § förordningen (2004:329) om bank- och finansieringsrörelse att föra ett bankregister för bankaktiebolag, sparbanker, medlemsbanker och utländska banker med filial i Sverige, och Finansinspektionens skyldighet enligt förordningen (2004:331) om valutaväxling och annan finansiell verksamhet att föra register över fysiska personer som har anmält att de avser att ägna sig åt valutaväxling i väsentlig omfattning eller annan finansiell verksamhet. Som ytterligare exempel kan nämnas skyldigheten för sådana verksamhetsutövare som avses i lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen) att behandla personuppgifter i syfte att förhindra att finansiell verksamhet och annan näringsverksamhet utnyttjas för penningtvätt eller finansiering av terrorism.

De uppgifter som myndigheter och privata aktörer har enligt författningarna på finansmarknadsområdet eller enligt beslut som har meddelats med stöd av sådana författningar är regelmässigt uppgifter av allmänt intresse. I vart fall utgör de rättsliga förpliktelser. För myndigheternas del innefattar uppgifterna dessutom ofta myndighetsutövning. Uppgifterna och förpliktelserna – och den myndighetsutövning som kan ligga i dem – är

fastställda i den nationella rätten och författningarna är proportionerliga i förhållande till den enskildes intresse av skydd för sin personliga integritet på det sätt som krävs enligt artikel 6.3 i dataskyddsförordningen. Nödvändig personuppgiftsbehandling får därför ske med stöd av artikel 6.1 första stycket c eller e i dataskyddsförordningen. Dataskyddsreformen medför alltså inte något behov av författningsändringar i detta avseende.

Det bör i detta sammanhang påpekas att även de övriga leden i artikel 6.1 första stycket i förekommande fall kan åberopas som rättsligt stöd för personuppgiftsbehandling på de nämnda rättsområdena.

Det bör också påpekas att den personuppgiftsansvarige är skyldig att försäkra sig om att den konkreta behandlingen sker lagligt, dvs. att det rör sig om nödvändig behandling med rättsligt stöd, och att övriga krav på personuppgiftsbehandlingen är uppfyllda.

5.2 Känsliga personuppgifter

Promemorians förslag: Hänvisningar i författningarna på finansmarknadsområdet till personuppgiftslagens bestämmelser om känsliga personuppgifter ska ersättas av hänvisningar till dataskyddsförordningen. I bestämmelserna i lagen och förordningen om registrering av verkliga huvudmän där det uttryckligen anges de typer av känsliga personuppgifter som omfattas av 13 § personuppgiftslagen ska det också införas hänvisningar till artikel 9.1 i dataskyddsförordningen.

Skälen för promemorians förslag

Personuppgiftslagens krav

Enligt 13 § PUL är det förbjudet att behandla s.k. känsliga personuppgifter, dvs. personuppgifter som rör hälsa eller sexualliv och personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening. Undantag från detta förbud finns i 15–19 §§ PUL.

Dataskyddsförordningens krav

I artikel 9.1 i dataskyddsförordningen finns, i likhet med PUL, ett generellt förbud mot behandling av känsliga personuppgifter (rubricerade som ”särskilda kategorier av personuppgifter” i dataskyddsförordningen). Enligt förordningen omfattar dessa personuppgifter emellertid även genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person och uppgifter om en fysisk persons sexuella läggning. Vidare finns i artikel 9.2 undantag från förbudet. Exempelvis är behandling tillåten i följande fall, vilka bedöms särskilt relevanta för författningarna på finansmarknadsområdet.

- 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 (artikel 9.2 c).
- Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade (artikel 9.2 e).
- Behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk eller som en del av domstolarnas dömande verksamhet (artikel 9.2 f).
- Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara 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 (artikel 9.2 g).

Vissa av undantagen, t.ex. det i artikel 9.2 g, hänvisar till nationell rätt. Enligt Dataskyddsutredningen talar mycket för att dessa undantag bör föreskrivas i nationell rätt. I vart fall anser utredningen att en sådan reglering inte är oförenlig med dataskyddsförordningen (SOU 2017:39 s. 162–165).

Dataskyddsutredningens förslag

Dataskyddsutredningen föreslår att det i den nya dataskyddslagen ska anges vissa generella undantag från förbudet att behandla känsliga personuppgifter, bl.a. för att möjliggöra behandling med hänsyn till viktiga allmänintressen (dvs. ett utflöde av artikel 9.2 g i dataskyddsförordningen). Utredningen föreslår i det avseendet att myndigheter ska få behandla känsliga personuppgifter i löpande text, om uppgifterna har lämnats in i ett ärende eller är nödvändiga för handläggningen av det, eller om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt någon annan lag. Dessutom ska myndigheter få behandla känsliga personuppgifter i enstaka fall om det är absolut nödvändigt för ändamålet med behandlingen och den inte innebär ett otillbörligt intrång i den registrerades personliga integritet. Därutöver föreslås att regeringen ska få meddela föreskrifter om ytterligare undantag från förbudet, om det behövs med hänsyn till ett viktigt allmänt intresse (3 kap. 3 och 8 §§ dataskyddslagen).

För att säkerställa nödvändiga och lämpliga skyddsåtgärder föreslår utredningen samtidigt att myndigheter som behandlar känsliga personuppgifter enbart med stöd av 3 kap. 3 § dataskyddslagen inte ska få använda sökbegrepp som avslöjar känsliga personuppgifter (3 kap. 4 § dataskyddslagen).

I penningtvättslagen bör hänvisningen till personuppgiftslagen i bestämmelserna om känsliga personuppgifter ersättas med en hänvisning till dataskyddsförordningen

Bestämmelser som hänvisar till 13 § PUL finns i 5 kap. 5 § penningtvättslagen.

Enligt 5 kap. 5 § första stycket får känsliga personuppgifter som avses i 13 § PUL behandlas under vissa förutsättningar. Sådan behandling får ske om det är nödvändigt för att bedöma om en kund till en sådan verksamhetsutövare som omfattas av lagen är en person i politiskt utsatt ställning eller familjemedlem eller känd medarbetare till en sådan person (punkt 1). Sådan behandling får även ske om det är nödvändigt för att bedöma den risk för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen (punkt 2) eller för att uppfylla skyldigheten

att övervaka pågående affärsförbindelser och bedöma enstaka transaktioner som är på visst sätt avvikande eller annars kan antas ingå som ett led i penningtvätt eller finansiering av terrorism (punkt 3). Vidare får känsliga personuppgifter behandlas om det är nödvändigt för att bedöma om det finns skälig grund att misstänka att det är fråga om penningtvätt eller finansiering av terrorism eller att egendom annars härrör från brottslig handling (punkt 4). Slutligen får behandling av känsliga personuppgifter ske om det är nödvändigt för att lämna uppgifter till Polismyndigheten enligt 4 kap. 3 § om omständigheter som kan tyda på penningtvätt eller finansiering av terrorism eller att egendom annars härrör från brottslig handling eller om det annars är nödvändigt för att lämna uppgifter enligt 4 kap. 6 § som behövs för en utredning om penningtvätt eller finansiering av terrorism (punkt 5).

Exemplen i 5 kap. 5 § första stycket är uttömmande. I andra stycket anges emellertid att känsliga personuppgifter också får behandlas vid en verksamhetsutövares bevarande av handlingar och uppgifter avseende åtgärder som har vidtagits för kundkännedom eller avseende vissa transaktioner (5 kap. 3 och 4 §§), om det är tillåtet att behandla uppgifterna enligt första stycket.

Enligt 5 kap. 8 § får en verksamhetsutövares register med uppgifter om misstänkt penningtvätt eller finansiering av terrorism inte samköras med motsvarande register hos någon annan.

Besked om att personuppgifter behandlas enligt 4 kap. 2, 3 eller 6 § och om att sådana uppgifter lagras enligt 5 kap. 3 eller 4 § får inte lämnas ut till den registrerade (5 kap. 7 §, se även avsnitt 7.2). Den som är verksam hos en verksamhetsutövare får inte obehörigen röja att personuppgifter behandlas enligt 5 kap. 5 och 6 §§ eller 4 kap. 2, 3 och 6 §§ och att sådana uppgifter bevaras enligt 3 och 4 §§ (5 kap. 11 §).

Behandling av känsliga personuppgifter som sker enligt 5 kap. 5 § bedöms vara nödvändig med hänsyn till ett viktigt allmänt intresse, och grunden för behandlingen finns i nationell rätt, som i sin tur är grundad på unionsrätten (Europaparlamentets och rådets direktiv [EU] 2015/849 av den 20 maj 2015 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism, om ändring av Europaparlamentets och rådets förordning [EU] nr 648/2012 och om upphävande av Europaparlamentets och rådets direktiv 2005/60/EG och

kommissionens direktiv 2006/70/EG [fjärde penningtvättsdirektivet], se bl.a. artikel 43). Det bedöms vara tillräckligt tydligt vilken behandling som är tillåten. Med hänsyn till att samkörning av register mellan olika verksamhetsutövare inte får ske och till att det råder tystnadsplikt för verksamma hos en verksamhetsutövare avseende känsliga personuppgifter finns det också lämpliga och särskilda skyddsåtgärder. Behandlingen är därför tillåten med stöd av artikel 9.2 g i dataskyddsförordningen. Det är därutöver möjligt att behandling av känsliga personuppgifter enligt 5 kap. 5 § kan vara tillåten på andra grunder enligt artikel 9.2.

Sammanfattningsvis är bestämmelserna om behandling av känsliga personuppgifter i 5 kap. 5 § penningtvättslagen förenliga med dataskyddsförordningen. Hänvisningen till 13 § PUL bör emellertid ersättas med hänvisning till artikel 9.1 i dataskyddsförordningen. Det kan i sammanhanget påpekas att behandlingen i det enskilda fallet måste leva upp till dataskyddsförordningens krav i övrigt, t.ex. principerna för behandling i artikel 5, för att vara tillåten.

I lagen om registrering av verkliga huvudmän bör det i bestämmelsen om att känsliga uppgifter inte behöver anges i en anmälan införas en hänvisning till dataskyddsförordningen

Enligt lagen (2017:631) om registrering av verkliga huvudmän är en juridisk person skyldig att anmäla uppgifter om vem som är dess verkliga huvudman till Bolagsverket (2 kap. 1 och 3 §§). Enligt 2 kap. 6 § gäller dock undantag från denna skyldighet i fråga om vissa närmare angivna känsliga uppgifter. Undantaget syftar till att undvika att känsliga personuppgifter enligt 13 § PUL behandlas i registret (prop. 2016/17:173 s. 570).

Exemplen på känsliga uppgifter i artikel 9.1 i dataskyddsförordningen är som nämns ovan något utökade i förhållande till 13 § PUL. För att undantaget i 2 kap. 6 § lagen om registrering av verkliga huvudmän ska stå i paritet med det som i dataskyddsförordningen avses med känsliga personuppgifter bör den bestämmelsen därför omfatta samma uppgifter som anges i artikel 9.1. Detta bör ske genom att en hänvisning till artikeln införs i bestämmelsen.

I förordningen om registrering av verkliga huvudmän bör det i bestämmelsen om sökord i register införas en hänvisning till dataskyddsförordningen

Enligt förordningen (2017:667) om registrering av verkliga huvudmän får uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv inte användas som sökbegrepp vid sökning i Bolagsverkets register över verkliga huvudmän (3 kap. 9 §). De uppgifter som nämns är samma som omfattas av 13 § PUL. Bestämmelsen bör i förhållande till dataskyddsförordningen omfatta vad som därutöver avses med känsliga personuppgifter i artikel 9.1. Detta bör ske genom att en hänvisning till artikeln införs i bestämmelsen.

5.3 Uppgifter om fällande domar i brottmål och överträdelser

Promemorians förslag: Hänvisningar i författningarna på finansmarknadsområdet till personuppgiftslagens bestämmelser om uppgifter om lagöverträdelser, domar i brottmål, straffprocessuella tvångsmedel och administrativa frihetsberövanden ska ersättas av hänvisningar till dataskyddsförordningen.

Promemorians bedömning: Bestämmelserna på finansmarknadsområdet om uppgifter om fällande domar i brottmål och överträdelser är förenliga med dataskyddsförordningen.

Skälen för promemorians förslag och bedömning

Personuppgiftslagens krav

Enligt 21 § PUL är det förbjudet för andra än myndigheter att behandla personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden. Förbudet gäller dock inte behandling för forskningsändamål, under vissa i paragrafen angivna förutsättningar. Vidare får regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om undantag från förbudet.

Regeringen får dessutom i enskilda fall besluta om undantag från förbudet samt överlåta åt tillsynsmyndigheten att fatta sådana beslut.

Dataskyddsförordningens krav

Enligt artikel 10 i dataskyddsförordningen får personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder endast behandlas 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 dock endast föras under kontroll av en myndighet. Artikeln har i stort samma lydelse som artikel 8.5 i dataskyddsdirektivet, även om tillämpningsområdet beträffande brottmålsdomar i förordningen begränsats till att enbart omfatta fällande sådana. Vidare är en betydande skillnad i förordningen jämfört med direktivet att det inte finns någon möjlighet för medlemsstaterna att med stöd av denna artikel begränsa behandlingen av personuppgifter om avgöranden i tvistemål och administrativa sanktioner.

Dataskyddsutredningens förslag

Dataskyddsutredningen föreslår att det i den nya dataskyddslagen ska anges att personuppgifter som rör fällande domar i brottmål, lagöverträdelser som innefattar brott eller straffprocessuella tvångsmedel får behandlas enligt artikel 10 i dataskyddsförordningen av myndigheter (3 kap. 9 § dataskyddslagen). Utredningen föreslår också att den myndighet som regeringen bestämmer i enskilda fall ska få meddela särskilda beslut om att tillåta behandling av sådana uppgifter (3 kap. 10 § dataskyddslagen).

Utredningen bedömer samtidigt att det inte finns stöd i dataskyddsförordningen att föreskriva ett förbud mot behandling av personuppgifter om administrativa frihetsberövanden (SOU 2017:39 s. 192–196).

Hänvisningar till personuppgiftslagen bör ersättas med hänvisningar till dataskyddsförordningen

I tre lagar på finansmarknadsområdet finns bestämmelser med hänvisningar till 21 § PUL. Två av dem finns i 2 kap. 12 § lagen (1991:980) om handel med finansiella instrument respektive 2 kap. 7 § lagen (2016:1306) med kompletterande bestämmelser till EU:s marknadsmissbruksförordning (förkortad LKMF). Båda bestämmelserna innebär undantag från förbudet i 21 § PUL.

I penningtvättslagen finns också en hänvisning till 21 § PUL med undantag från förbudet under vissa angivna förutsättningar (5 kap. 6 §).

Lagen om handel med finansiella instrument

Inför upprättandet och offentliggörandet av ett emissionsprospekt får, utan hinder av 21 § PUL, sådana personuppgifter behandlas som prospektet ska innehålla (2 kap. 12 § lagen om handel med finansiella instrument). I den utsträckning det krävs enligt bestämmelserna om hur prospektet ska offentliggöras (2 kap. 28–30 §§) får personuppgifterna i prospektet föras över till en stat utanför EES. Bestämmelserna har införts mot bakgrund av att det i kommissionens förordning (EG) nr 809/2004 av den 29 april 2004 om genomförande av Europaparlamentets och rådets direktiv 2003/71/EG i fråga om informationen i prospekt, utformningen av dessa, införlivande genom hänvisning samt offentliggörande av prospekt och spridning av annonser (prospektförordningen) ställs upp ett krav på att uppgifter om personer i ledande befattning som har dömts i bedrägerirelaterade mål under de senaste fem åren ska finnas med i prospektet, som bl.a. ska göras tillgängligt på en elektronisk hemsida (jfr prop. 2004/05:158 s. 176).

Krav på prospektets innehåll finns i övrigt i 2 kap. 11 § lagen om handel med finansiella instrument. Enligt 2 kap. 19 § får Finansinspektionen i ett enskilt fall besluta om att information som krävs enligt 2 kap. 11 § eller prospektförordningen får utelämnas bl.a. om offentliggörande skulle innebära allvarlig skada för emittenten och utelämnande inte kan antas medföra att allmänheten vilseleds. Bestämmelsen medger dock inte att hänsyn kan tas till en fysisk person som uppgiften rör. Finansinspektionen får även besluta att

information får utelämnas om den är av mindre betydelse och inte skulle påverka bedömningen beträffande den finansiella ställningen hos och framtidsutsikterna för emittenten, den som lämnar erbjudandet eller en eventuell garant.

Det är bara inför upprättandet av prospektet, och vid offentliggörandet av det, som undantaget i 2 kap. 12 § gäller. Bestämmelsen ger alltså inte stöd för en fortlöpande registrering av ledande personers brottslighet, utan det är bara när det har blivit aktuellt att upprätta ett prospekt som de uppgifter som prospektet ska innehålla får samlas in och behandlas i övrigt i syfte att upprätta och offentliggöra prospektet (se samma prop.).

Behandling av personuppgifter utan hinder av 21 § PUL enligt 2 kap. 12 § lagen om handel med finansiella instrument är således tillåten enligt såväl unionsrätten som nationell rätt och är, genom Finansinspektionens möjlighet att besluta om att viss information får utelämnas, i viss mening under myndighets kontroll. Eftersom bestämmelsen inte ger stöd för en fortlöpande registrering av ledande personers brottslighet utan endast behandling inför upprättande och offentliggörande av prospektet blir bestämmelsen proportionerlig i förhållande till sitt syfte. Bestämmelsen i 2 kap. 12 § lagen om handel med finansiella instrument bedöms mot denna bakgrund vara förenlig med dataskyddsförordningen. Hänvisningen till 21 § PUL bör dock ersättas med en hänvisning till artikel 10 i dataskyddsförordningen.

Lagen med kompletterande bestämmelser till EU:s marknadsmissbruksförordning

Enligt LKMF ska ett finansiellt företag tillhandahålla ändamålsenliga rapporteringssystem för anställda som vill göra anmälningar om misstänkta överträdelser av marknadsmissbruksförordningen (2 kap. 7 § första stycket). PUL gäller vid behandling av personuppgifter inom ramen för sådana rapporteringssystem. Uppgifter om lagöverträdelser som avses i 21 § PUL får dock behandlas om uppgifterna avser brott enligt lagen (2016:1307) om straff för marknadsmissbruk på värdepappersmarknaden (2 kap. 7 § andra stycket LKMF).

Det finns flera bestämmelser på finansmarknadsområdet som ställer krav på att aktörer ska tillhandahålla rapporteringssystem för

s.k. visselblåsande. I samtliga dessa bestämmelser, utom 2 kap. 7 § LKMF, anges att PUL gäller vid behandling av personuppgifter för sådana system, utan undantag. I fråga om LKMF har det dock ansetts nödvändigt med ett undantag från 21 § PUL för att leva upp till marknadsmissbruksförordningens krav.

Enligt marknadsmissbruksförordningen ska medlemsstaterna kräva att arbetsgivare som utför verksamhet som styrs av reglering avseende finansiella tjänster inför lämpliga interna förfaranden för att deras anställda ska kunna rapportera överträdelser av den förordningen. I den mån detta innebär behandling av personuppgifter avseende brott aktualiserar det förbudet i 21 § PUL. Överträdelser av marknadsmissbruksförordningen utgör dock inte brott utan administrativa överträdelser. Förbudet i 21 § PUL är därför inte tillämpligt på personuppgifter som rör överträdelser av förordningen. Däremot kan överträdelser av förbuden mot marknadsmissbruk (insiderhandel, marknadsmanipulation och olagligt röjande av insiderinformation) i förordningen samtidigt utgöra brott enligt lagen om straff för marknadsmissbruk på värdepappersmarknaden. Bestämmelserna i PUL torde enligt förarbetena till LKMF därför innebära att företag är förhindrade att behandla personuppgifter som rör överträdelser av motsvarande förbud i marknadsmissbruksförordningen (prop. 2016/17:22 s. 318–321).

Datainspektionen har med stöd av 9 § PUF meddelat föreskrifter om undantag från förbudet i 21 § PUL, bl.a. för att möjliggöra användning av visselblåsarsystem (Datainspektionens föreskrifter [DIFS 2010:1] om ändring av Datainspektionens föreskrifter [DIFS 1998:3] om undantag från förbudet för andra än myndigheter att behandla personuppgifter om lagöverträdelser m.m.). Föreskrifterna medger att uppgifter om bl.a. brottslighet inom bank- och finansväsen behandlas, men enbart om uppgifterna avser personer i nyckelpositioner eller ledande ställning inom det egna bolaget eller koncernen.

För att kunna upprätthålla ändamålsenliga rapporteringssystem har det ansetts att det bör vara möjligt för de aktuella företagen att behandla sådana uppgifter som rör misstänkt marknadsmissbruk även avseende andra än nyckelpersoner. Mot denna bakgrund har därför undantaget från 21 § PUL införts i LKMF i anslutning till

bestämmelsen om interna rapporteringssystem (samma prop. s. 320 f.).

Med hänsyn till att det rör sig om uppgifter som är känsliga för den enskilde och mot bakgrund av dataskyddsförordningens krav om lämpliga skyddsåtgärder har det i LKMF införts en bestämmelse om tystnadsplikt i 2 kap. 8 § för den som är eller har varit anställd hos ett finansiellt företag avseende uppgifter i en anmälan eller utsaga som gjorts till ett sådant rapporteringssystem som avses i 2 kap. 7 § om uppgiften kan avslöja anmälarens eller den utpekade personens identitet, samt en motsvarande sekretessbestämmelse för sådan uppgift i en statlig myndighets verksamhet i 30 kap. 6 b § offentlighets- och sekretesslagen (2009:400) (se vidare avsnitt 7.2). I likhet med bestämmelsen om tystnadsplikt i lagen om värdepapperscentraler och kontoföring av finansiella instrument omfattar tystnadsplikten när det gäller finansiella företags interna system för rapportering av misstänkta överträdelser av marknadsmissbruksförordningen endast skydd för obehörigt röjande. Med det avses t.ex. inte att uppgifter lämnas på begäran av Finansinspektionen eller åklagaren (samma prop. s. 321).

Behandling av personuppgifter enligt 2 kap. 7 § LKMF har således stöd i nationell rätt. Möjligheten till behandling enligt bestämmelsen av personuppgifter om lagöverträdelser som innefattar brott är införd för att marknadsmissbruksförordningens krav på rapporteringssystem för visselblåsare ska kunna uppfyllas och får anses proportionerlig i förhållande till sitt syfte. Genom nuvarande bestämmelser om tystnadsplikt finns det lämpliga skyddsåtgärder. Hänvisningen till 21 § PUL bör dock ersättas med en hänvisning till artikel 10 i dataskyddsförordningen.

Penningtvättslagen

Enligt penningtvättslagen (5 kap. 6 § första stycket) får personuppgifter om lagöverträdelser som avses i 21 § PUL behandlas endast om det är nödvändigt för att bedöma den risk som kan förknippas med en kundrelation enligt 2 kap. 3 § (risk för penningtvätt eller finansiering av terrorism), för att uppfylla skyldigheten att övervaka pågående affärsförbindelser m.m. enligt 4 kap. 1 §, för att bedöma misstänkta transaktioner och aktiviteter

enligt 4 kap. 2 § och för att lämna uppgifter till Polismyndigheten enligt 4 kap. 3 och 6 §§. Uppgifter om lagöverträdelser får enligt 5 kap. 6 § andra stycket också behandlas vid visst bevarande av handlingar om det är tillåtet att behandla uppgifterna enligt första stycket.

Bestämmelserna syftar till att verksamhetsutövare ska kunna behandla personuppgifter på ett sätt som gör det möjligt för dem att uppfylla skyldigheterna enligt det fjärde penningtvättsdirektivet (prop. 2016/17:173 s. 306–314). Behandlingen av personuppgifter om lagöverträdelser begränsas, i likhet med övrig personuppgiftsbehandling som regleras i penningtvättslagen, av bestämmelsen som anger syftet med personuppgiftsbehandlingen. En behandling av personuppgifterna för annat syfte kan medföra skadeståndsskyldighet eller straffansvar. Det bör vidare beaktas att bestämmelsen om behandling av personuppgifter om lagöverträdelser till stor del endast innebär ett förtydligande av det rättsläge som ansetts föreligga även utan sådan särskild reglering (jfr prop. 2014/15:80 s. 43 f.).

Sammanfattningsvis är bestämmelserna i penningtvättslagen som tillåter behandling av personuppgifter enligt 21 § PUL förenliga med dataskyddsförordningen. Hänvisningarna till 21 § PUL bör dock ersättas med hänvisningar till artikel 10 i dataskyddsförordningen.

6 Personuppgiftsansvariga och personuppgiftsbiträden

6.1 Personuppgiftsansvarigas roll

Liksom i dataskyddsdirektivet förutsätts i dataskyddsförordningen att det finns en personuppgiftsansvarig (i direktivet används dock termen registeransvarig) för all personuppgiftsbehandling. Med personuppgiftsansvarig avses den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Om ändamålen med 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 den nationella rätten (artikel 4.7 i dataskyddsförordningen).

Med uppgiften som personuppgiftsansvarig följer vissa skyldigheter enligt dataskyddsförordningen. Dessa skyldigheter är till stora delar desamma som i dataskyddsdirektivet. Även dataskyddsförordningen kräver till exempel att den personuppgiftsansvarige ser till att behandlingen av personuppgifter sker på ett korrekt och säkert sätt (artikel 5.2), att oriktiga uppgifter rättas (artikel 16) och att den registrerade ersätts för skada som en rättsstridig behandling av personuppgifter har medfört (artikel 82).

En nyhet i dataskyddsförordningen är kravet i artikel 26 på att gemensamt personuppgiftsansvariga ska ha ett inbördes arrangemang. Enligt artikeln ska gemensamt personuppgiftsansvariga fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt förordningen, såvida inte deras respektive skyldigheter fastställs genom unionsrätten eller den nationella rätt som de omfattas av. Arrangemanget ska återspegla de gemensamt personuppgiftsansvarigas roller och förhållanden gentemot de registrerade. Oavsett arrangemang får dock den registrerade utöva sina

rättigheter enligt förordningen med avseende på, och emot, var och en av de personuppgiftsansvariga.

En annan nyhet är att den personuppgiftsansvarige (och personuppgiftsbiträdet, se nedan) i större utsträckning än i dag är skyldig att utse ett dataskyddsombud (i direktivet används termen uppgiftsskyddsombud). Till exempel blir det obligatoriskt för i princip samtliga myndigheter att ha ett sådant ombud (artikel 37). I sammanhanget kan det nämnas att dataskyddsombudets ställning stärks, bl.a. genom att ombudet ska rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbiträdets högsta förvaltningsnivå och att ombudet inte får tilldelas arbetsuppgifter som leder till en intressekonflikt (artikel 38).

6.2 Personuppgiftsbiträdenas roll

Dataskyddsförordningen medför något större förändringar för personuppgiftsbiträdena (i dataskyddsdirektivet används termen registerförare). Definitionen av personuppgiftsbiträde är i sak densamma som definitionen av registerförare i dataskyddsdirektivet, nämligen den som behandlar personuppgifter för den personuppgiftsansvariges räkning (artikel 4.8 i dataskyddsförordningen). Mer långtgående skyldigheter för personuppgiftsbiträdet införs emellertid genom dataskyddsförordningen. Till exempel får biträdet inte anlita underbiträden utan tillstånd från den personuppgiftsansvarige (artikel 28.2). Vidare ställs det upp nya krav på det avtal eller den rättsakt som reglerar biträdets personuppgiftsbehandling (se artikel 28.3). Personuppgiftsbiträdet ska vidare, tillsammans med den personuppgiftsansvarige, i tillämpliga fall utse dataskyddsombudet (artikel 37).

Av särskild betydelse är att det genom dataskyddsförordningen införs egna skyldigheter för personuppgiftsbiträdena. Till exempel är biträdet skyldigt att ha en godtagbar säkerhetsnivå (artikel 32). Vidare kan ett biträde under vissa förutsättningar bli skyldig att betala ersättning till den registrerade vid felaktig personuppgiftsbehandling (artikel 82).

6.3 Bestämmelser om personuppgiftsansvaret

Promemorians förslag: Hänvisningar till personuppgiftslagen i bestämmelser på finansmarknadsområdet som pekar ut en personuppgiftsansvarig ska tas bort.

Promemorians bedömning: Bestämmelser om vem som är personuppgiftsansvarig bör behållas. Författningar som pekar ut den registerförande myndigheten men inte den som är personuppgiftsansvarig behöver däremot inte kompletteras med bestämmelser om vem som är personuppgiftsansvarig.

Skälen för promemorians förslag och bedömning

Bestämmelser som pekar ut en personuppgiftsansvarig kan behållas

Bestämmelser på finansmarknadsområdet som pekar ut en personuppgiftsansvarig enligt PUL finns i bl.a. 4 kap. 1 § lagen (1998:1479) om värdepapperscentraler och kontoföring av finansiella instrument (kontoföringslagen), 1 § lagen (1999:889) om registrering av krigsskada på egendom, 6 § förordningen (2004:330) om inlåningsverksamhet och 2 kap. 3 § LKMF. För dessa register bestäms ändamålen med och medlen för behandlingen i författning (se t.ex. 4 kap. 1 § kontoföringslagen).

De nämnda bestämmelserna om personuppgiftsansvar bedöms i sig förenliga med dataskyddsförordningen, eftersom det enligt artikel 4.7 är tillåtet att peka ut vem som är personuppgiftsansvarig i nationell lagstiftning. Hänvisningarna till PUL bör dock tas bort. Det är inte nödvändigt att ersätta hänvisningarna till PUL med hänvisningar till dataskyddsförordningen. Bestämmelserna behöver inte heller kompletteras med mer detaljerade uppgifter om vem som är personuppgiftsansvarig.

I författningar där det inte pekas ut vem som är den personuppgiftsansvarige behöver det inte införas några kompletterande bestämmelser

Det finns också författningar där det pekas ut vem som ska föra ett visst register eller en förteckning över vissa uppgifter, utan att

uttryckligen peka ut den personuppgiftsansvarige. Som exempel kan nämnas lagen om värdepappersmarknaden, där det i 6 kap. 7 § föreskrivs att Bolagsverket för register över anknutna ombud, där de uppgifter som enligt lag eller andra författningar ska tas in i register skrivs in. Både ändamålen med och medlen för behandlingen bestäms i författningen (se 6 kap. 1 §). Detta möjliggör enligt artikel 4.7 i dataskyddsförordningen att det i nationell rätt föreskrivs vem som är personuppgiftsansvarig. Att den personuppgiftsansvarige får pekas ut i nationell rätt betyder emellertid inte att så måste ske. De berörda författningarna behöver därför inte kompletteras med uppgift om vem som är personuppgiftsansvarig.

7 Den registrerades rättigheter

7.1 Rättigheterna enligt dataskyddsförordningen och dataskyddslagen

I dataskyddsförordningens tredje kapitel behandlas den registrerades rättigheter. Kapitlet avser rätten till information (artiklarna 13 och 14) och tillgång till bl.a. registerutdrag (artikel 15). Vidare behandlas rätten till rättelse (artikel 16), radering (artikel 17), begränsning av behandling (artikel 18) och dataportabilitet (artikel 20). Slutligen behandlas rätten att göra invändningar (artikel 21) och att motsätta sig automatiskt individuellt beslutsfattande (artikel 22). I anslutning till dessa rättigheter finns bestämmelser om hur och när information ska lämnas (artikel 12) och bestämmelser om anmälningsskyldighet för det fall rättelse, radering eller begränsning av behandling sker (artikel 19).

Bestämmelserna om den registrerades rättigheter, med motsvarande skyldigheter för den personuppgiftsansvarige, är direkt tillämpliga. Rättigheterna är emellertid inte absoluta utan kan enligt artikel 23 i dataskyddsförordningen begränsas under vissa, i artikeln angivna, förutsättningar.

Dataskyddsutredningen föreslår att det i den nya dataskyddslagen görs undantag från informationsskyldigheten enligt artiklarna 13–15 i dataskyddsförordningen, om sekretess eller tystnadsplikt föreligger (5 kap. 1 § dataskyddslagen). Utredningen föreslår vidare att den registrerades rätt till registerutdrag som huvudregel inte ska omfatta personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande (5 kap. 2 § dataskyddslagen). Slutligen föreslår utredningen ett generellt bemyndigande för regeringen att meddela

föreskrifter om ytterligare begränsningar enligt artikel 23 i dataskyddsförordningen (5 kap. 3 § dataskyddslagen).

7.2 Bestämmelser om tystnadsplikt

Promemorians bedömning: Bestämmelser om tystnadsplikt angående personuppgifter på finansmarknadsområdet är förenliga med dataskyddsförordningen och bör stå kvar oförändrade.

Promemorians förslag: Hänvisning till personuppgiftslagen ska ersättas med hänvisning till dataskyddsförordningen.

Skälen för promemorians bedömning och förslag

Allmänt om undantag från rätt till information vid lagstadgad tystnadsplikt

Den personuppgiftsansvariges skyldighet att självmant tillhandahålla den registrerade information om behandlingen av personuppgifter följer av artiklarna 13 och 14 i dataskyddsförordningen. Motsvarande regler, om än inte lika utförliga, finns i artiklarna 10 och 11 i dataskyddsdirektivet, vilka i svensk rätt har genomförts genom 23–25 §§ PUL. Den registrerade har vidare enligt artikel 15 i dataskyddsförordningen rätt att på begäran få information om och tillgång till de personuppgifter som behandlas (s.k. registerutdrag).

I artikel 14.5 i dataskyddsförordningen föreskrivs flera direkt tillämpliga undantag från rätten till information angående uppgifter insamlade från annan än den registrerade, bl.a. om personuppgifterna måste förbli konfidentiella till följd av tystnadsplikt enligt unionsrätt eller nationell rätt, inbegripet lagstadgade sekretessförpliktelser (led d). I artikel 15.4 anges endast att rätten till registerutdrag (kopia av de personuppgifter som är under behandling) inte ska påverka menligt på andras friheter och rättigheter. Bestämmelsen i artikel 23 möjliggör dock ytterligare undantag på samma sätt som dataskyddsdirektivet (jfr SOU 2017:39 s. 205).

Enligt artikel 23.1 i dataskyddsförordningen ska det vara möjligt att i unionsrätten eller i en medlemsstats nationella rätt begränsa

tillämpningsområdet för de skyldigheter och rättigheter som föreskrivs i bl.a. artiklarna 13–15, 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 bl.a. den nationella eller allmänna säkerheten (artikel 23.1 a respektive c) eller 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 (artikel 23.1 d). Vidare gäller rätt till sådana undantag i syfte att säkerställa andra av unionens eller en medlemsstats viktiga mål av generellt allmänt intresse, särskilt ett av unionens eller en medlemsstats viktiga ekonomiska eller finansiella intressen (artikel 23.1 e). Ett annat syfte som omfattas av möjligheten till undantagsbestämmelser är säkerställande av skydd av den registrerades eller andras rättigheter och friheter (23.1 i).

Av det direkt tillämpliga undantaget i artikel 14.5 d i dataskyddsförordningen följer alltså att den personuppgiftsansvarige inte på eget initiativ behöver förse den registrerade med information angående uppgifter insamlade från annan än den registrerade så snart uppgifterna omfattas av lagstadgad tystnadsplikt. Dataskyddsutredningen anser det behövligt att klargöra att sådan tystnadsplikt också kan medföra att en begäran från den registrerade om bekräftelse och information enligt artikel 15 ska avslås. Mot denna bakgrund föreslår utredningen, som nämns i avsnitt 7.1, att det i den nya dataskyddslagen anges en generell bestämmelse om att den registrerades rätt till information och tillgång till uppgifter enligt artiklarna 13–15 inte gäller 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. Den nuvarande generella bestämmelsen om sådant undantag finns i 27 § PUL.

Mot bakgrund av att Dataskyddsutredningen bedömer att rättsläget när det gäller möjligheten att begränsa den registrerades rätt till information och tillgång till uppgifter inte förändras i och med dataskyddsförordningen föreslår utredningen att den nya bestämmelsen ska motsvara nuvarande 27 § PUL i dess helhet. Dataskyddsutredningen bedömer på samma sätt att förarbetsuttalanden och praxis rörande 27 § PUL bör kunna vara vägledande även vid

tillämpningen av den nya bestämmelsen (se samma betänkande s. 204–206).

Bestämmelser på finansmarknadsområdet om tystnadsplikt avseende personuppgifter

Tystnadsplikt avseende visselblåsning

I flera författningar på finansmarknadsområdet finns i dag bestämmelser om sådan tystnadsplikt som enligt 27 § PUL och bestämmelsen i 5 kap. 1 § dataskyddslagen som Dataskyddsutredningen föreslår ska gälla framför den registrerades rättigheter enligt artiklarna 13–15 i dataskyddsförordningen.

I flera författningar finns bestämmelser om tystnadsplikt till skydd för s.k. visselblåsare. Innebörden av dessa är att uppgift i en anmälan eller en utsaga om en misstänkt överträdelse av en bestämmelse som gäller för verksamheten hos t.ex. en värdepapperscentral, ett fondbolag, ett kreditinstitut eller ett annat finansiellt företag, inte får obehörigen röjas om uppgiften kan avslöja anmälarens identitet. Enligt fyra författningar gäller dessutom tystnadsplikt avseende uppgifter som kan avslöja den anmälde (ibland ”den utpekade”) personens identitet (8 kap. 2 § kontoföringslagen, 2 kap. 8 § LKMF, 1 kap. 11 § lagen om värdepappersmarknaden och 20 § lagen [2017:317] med kompletterande bestämmelser till EU:s förordning om faktablad för Priip-produkter). Sekretess avseende den anmälde personen är motiverad av integritetsskäl (prop. 2015/16:10 s. 226, prop. 2016/17:22 s. 329, prop. 2016/17:78 s. 57 och prop. 2016/17:162 s. 517). Tystnadsplikten enligt dessa bestämmelser avser endast skydd för obehörigt röjande. Med obehörigt röjande avses t.ex. inte att uppgifter lämnas på begäran av behöriga utredande myndigheter (se t.ex. prop. 2016/17:22 s. 321).

Övriga bestämmelser om tystnadsplikt

Utöver bestämmelser om tystnadsplikt i förhållande till visselblåsning finns ytterligare regler om tystnadsplikt med verkan mot en registrerad i 8 kap. 4 § kontoföringslagen, samt i 4 kap. 14 §

försäkringsrörelselagen (2010:2043). Även i penningtvättslagen finns sådana bestämmelser om tystnadsplikt (se nedan).

Bestämmelsen i 8 kap. 4 § kontoföringslagen ger en undersökningsledare eller åklagare som begär uppgifter från en svensk värdepapperscentral, eller ett kontoförande institut, om enskildas förhållanden enligt 8 kap. 2 a § samma lag, rätt att besluta att värdepapperscentralen eller det kontoförande institutet samt värdepapperscentralens eller institutets styrelseledamöter och anställda inte får röja för kunden eller för någon utomstående att uppgifter har lämnats eller att det pågår en förundersökning eller ett ärende om rättslig hjälp i brottmål.

Penningtvättslagen innehåller en huvudregel om tystnadsplikt gentemot bl.a. en kund hos en verksamhetsutövare angående verksamhetsutövarens bedömning om det finns skälig grund att misstänka att transaktioner eller andra aktiviteter utgör penningtvätt eller finansiering av terrorism eller att egendom annars härrör från brottslig handling (4 kap. 9 §). Samma tystnadsplikt gäller angående att verksamhetsutövaren lämnar uppgifter om sådana misstankar till Polismyndigheten enligt 4 kap. 3 eller 6 §.

Enligt 5 kap. 7 § penningtvättslagen får besked om att personuppgifter behandlas avseende sådana åtgärder som nämns ovan och om att sådana uppgifter lagras inte lämnas ut till den registrerade. Tystnadsplikt enligt 5 kap. 11 § penningtvättslagen innebär att den som är verksam hos en verksamhetsutövare inte obehörigen får röja att känsliga personuppgifter eller personuppgifter om lagöverträdelser behandlas enligt samma lag.

Bestämmelsen i 4 kap. 14 § försäkringsrörelselagen stadgar att en personuppgift som anger att en försäkringstagare har vidtagit dispositioner beträffande försäkringsbelopp som utfaller i framtiden till förmån för någon annan och som behandlas enligt PUL inte får lämnas ut till förmånstagaren.

Förhållandet till dataskyddsförordningen

I så måtto att ovan nämnda begränsningar av den registrerades rätt till information grundar sig i bestämmelser om lagstadgad tystnadsplikt är de förenliga med det direkt tillämpliga undantaget i artikel 14.5 d i dataskyddsförordningen från den personuppgifts-

ansvariges skyldighet att på eget initiativ informera den registrerade. Att därutöver låta bestämmelserna innebära undantag från den registrerades rätt till bekräftelse och information enligt artikel 15, liksom den registrerades rätt till information om behandling avseende uppgifter insamlade från den registrerade själv enligt artikel 13, förutsätter att ett sådant undantag är förenligt med förordningens bestämmelser om begränsningar av den registrerades rättigheter enligt artikel 23 (bortsett från att artikel 15.4 som nämns ovan stadgar om att en rätt till registerutdrag inte får inverka menligt på andras rättigheter och friheter). Att nu nämnda sektorsspecifika undantag är förenliga med dataskyddsförordningen är naturligtvis också en förutsättning för att den generella bestämmelsen i 5 kap. 1 § dataskyddslagen som Dataskyddsutredningen föreslår i sin tur ska vara förenlig med förordningen i dessa fall.

Som konstaterats ovan förutsätter undantag genom tystnadsplikt från den registrerades rätt till bekräftelse och information enligt artikel 15, liksom den registrerades rätt till information om behandling avseende uppgifter insamlade från den registrerade själv enligt artikel 13, att ett sådant undantag är förenligt med förordningens bestämmelser om begränsningar av den registrerades rättigheter.

Bestämmelserna om tystnadsplikt angående visselblåsning kan innebära att någon som blivit utpekad av en anmälare inte har rätt att begära ut information om denna personuppgiftsbehandling i den mån denna information kan avslöja anmälarens identitet. I de fyra författningar som nämns ovan där även den anmäldes identitet skyddas av sekretess är det inte skäl för sekretess gentemot den anmälde eftersom sådan sekretess endast motiveras av integritetsskäl, och inte t.ex. utredningsskäl. Av naturliga skäl gäller inte sekretess avseende den anmäldes identitet gentemot anmälaren heller. I den mån tredje mans personuppgifter behandlas i samband med en anmälan kan dock sekretess avseende såväl den utpekades som anmälarens identitet hindra att tredje man har rätt att begära ut information om behandlingen.

Samtliga nuvarande bestämmelser i svensk rätt på finansmarknadsområdet om tystnadsplikt i förhållande till visselblåsning har sin grund i unionsrätten (se bl.a. Europaparlamentets och rådets förordning [EU] nr 909/2014 av den 23 juli 2014 om förbättrad

värdepappersavveckling i Europeiska unionen och om värdepappers-centraler samt ändring av direktiv 98/26/EG och 2014/65/EU och förordning [EU] nr 236/2012, samt direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG och 2006/49/EG). Bestämmelserna till skydd för anmälaren – visselblåsaren – syftar bl.a. till att säkra viktiga mål av allmänt intresse för såväl unionen som Sverige. Eftersom en anmälan eller utsaga om en misstänkt överträdelse av bestämmelser som gäller för de berörda verksamheterna kan avse såväl brott som överträdelse av gällande etiska regler aktualiserar bestämmelserna även undantagen i artikel 23.1 d och g i dataskyddsförordningen. Tystnadsplikt till skydd för den anmäldes integritet faller under artikel 23.1 om skydd för den registrerades rättigheter och friheter. Bestämmelserna om tystnadsplikt avseende visselblåsning bedöms respektera andemeningen i de grundläggande rättigheterna och friheterna och utgöra nödvändiga och proportionella åtgärder i ett demokratiskt samhälle, samt leva upp till de övriga kraven i artikel 23.2. Med hänsyn till detta, samt till att nuvarande bestämmelser ansetts vara förenliga med dataskyddsdirektivet, bör de kvarstå oförändrade.

När det gäller bestämmelserna om tystnadsplikt i kontoföringslagen och penningtvättslagen kan det först konstateras att även om tystnadsplikten enligt dessa bestämmelser avser att främja utredning av brott etc. rör bestämmelserna andra än behöriga brottsutredande myndigheter, varför bestämmelserna inte faller utanför dataskyddsförordningens tillämpningsområde. Genom sina syften går det vidare att konstatera att bestämmelserna gör flera av bestämmelserna om begränsningar i artikel 23.1 i dataskyddsförordningen tillämpliga, såsom 23.1 d avseende förebyggande och utredande av brott m.m. När det gäller penningtvättslagen aktualiseras också bestämmelserna i 23.1 a och c avseende den nationella respektive den allmänna säkerheten. Även bestämmelsen i 23.1 e angående andra viktiga mål av generellt allmänt intresse aktualiseras. Bestämmelserna om tystnadsplikt i kontoföringslagen och penningtvättslagen bedöms respektera andemeningen i de grundläggande rättigheterna och friheterna och utgöra nödvändiga och proportionella åtgärder i ett demokratiskt samhälle, samt leva

upp till de övriga kraven i artikel 23.2 i dataskyddsförordningen. Med hänsyn till detta bör de kvarstå oförändrade.

Tystnadsplikten enligt 4 kap. 14 § försäkringsrörelselagen kan sägas utgöra ett skydd för försäkringstagarens rätt att hålla sådana dispositioner som avses i bestämmelsen hemliga för förmånstagaren, vilken aktualiserar begränsningsbestämmelsen i artikel 23.1 i i dataskyddsförordningen om skydd för den registrerades eller andras rättigheter och friheter. Bestämmelsen bedöms liksom de ovan nämnda bestämmelserna i övrigt vara förenlig med dataskyddsförordningen. Hänvisningen till PUL ska emellertid ersättas med en hänvisning till dataskyddsförordningen.

7.3 Andra bestämmelser om registerutdrag

Promemorians bedömning: Bestämmelser på finansmarknadsområdet som tillåter att ett registerutdrag begränsas till sitt innehåll i fråga om uppgifter som den enskilde redan har tagit del av kan behållas.

Promemorians förslag: Hänvisningar till personuppgiftslagen i bestämmelser om information om uppgifter i handlingar som den registrerade redan har tagit del av ska ersättas med hänvisningar till dataskyddsförordningen.

Skälen för promemorians bedömning

Personuppgiftslagen

Enligt 26 § PUL är den personuppgiftsansvarige skyldig att till var och en som ansöker om det en gång per år och utan kostnad lämna besked om huruvida personuppgifter som rör den sökande behandlas eller inte. Om sådana uppgifter behandlas, ska dessutom viss ytterligare information lämnas. Detta brukar kallas rätten till registerutdrag.

Dataskyddsförordningen

Att den registrerade ska ha rätt att få en bekräftelse på huruvida personuppgifter som rör honom eller henne behandlas och, om så är fallet, även få viss ytterligare information, följer av artikel 15 i dataskyddsförordningen. Till skillnad från bestämmelserna om den personuppgiftsansvariges skyldighet att självmant informera den registrerade om personuppgiftsbehandling i artiklarna 13 och 14 innehåller bestämmelserna om rätten till registerutdrag i artikel 15 inte något undantag när det gäller information som den registrerade redan förfogar över. I stället gäller enligt artikel 15.3 att den personuppgiftsansvarige ska förse den registrerade med en kopia av de personuppgifter som är under behandling och att den personuppgiftsansvarige för eventuella ytterligare kopior får ta ut en rimlig avgift. Som nämns ovan är emellertid rättigheterna enligt artikel 15 sådana som omfattas av de möjligheter till begränsningar som följer av artikel 23. Av betydelse är därutöver artikel 12.3, som får tolkas så att den personuppgiftsansvarige ska lämna registerutdraget till den registrerade utan onödigt dröjsmål och under alla omständigheter senast en månad efter den registrerades begäran. Perioden får under vissa förutsättningar förlängas.

Författningarna på finansmarknadsområdet

Hänvisningar till rätten till registerutdrag enligt PUL finns i 4 kap. 8 a § förordningen om bank- och finansieringsrörelse och i 3 kap. 6 § förordningen om registrering av verkliga huvudmän. I dessa bestämmelser anges att sådan information som ska lämnas enligt 26 § PUL inte behöver omfatta uppgifter i vissa handlingar, om den enskilde har tagit del av handlingens innehåll. I ett sådant fall ska det i stället framgå av informationen att handlingen behandlas av myndigheten. Om den enskilde begär det, ska dock informationen även omfatta uppgifterna i en sådan handling. Det är Bolagsverket som är personuppgiftsansvarigt för de register som bestämmelserna rör.

Med hänsyn till att den registrerade genom nämnda bestämmelser inte är betagen möjligheten att mot begäran få tillgång till personuppgifter som denne har tagit del av, bedöms bestämmelserna inte innebära någon egentlig inskränkning av

rätten att få tillgång till personuppgifter enligt artikel 15 i dataskyddsförordningen. För det fall att möjligheten att initialt utelämna uppgifter som den registrerade redan tagit del av skulle anses som en begränsning i förhållande till artikel 15, kan den hänsyn till den administrativa bördan för den personuppgiftsansvariga myndigheten (Bolagsverket) som ligger bakom bestämmelserna likväl åberopas som skäl för en begränsning i enlighet med artikel 23.1 e, dvs. som en begränsning med hänsyn till ett viktigt mål av generellt allmänt intresse. Särskilt med hänsyn till att den registrerade alltid har rätt att vid uttrycklig begäran få ut uppgifterna, måste möjligheten att initialt utelämna dem anses som en proportionerlig åtgärd i förhållande till detta syfte (jfr Ds 2017:19 s. 133–136 och Ds 2017:28 s. 146–150). Hänvisningarna till 26 § PUL behöver dock ersättas med hänvisning till artikel 15 i dataskyddsförordningen.

7.4 Rätten till rättelse

7.4.1 Gällande rätt

Rättelse enligt dataskyddsdirektivet

I artikel 12 b i dataskyddsdirektivet stadgas en rätt till rättelse för den registrerade. I artikel 13.1 finns regler om undantag från denna rättighet. Artikel 6.1 d i direktivet innehåller därtill en skyldighet för medlemsstaterna att föreskriva att personuppgifter ska vara riktiga och om nödvändigt aktuella, samt en skyldighet att vidta alla rimliga åtgärder för att säkerställa att personuppgifter som är felaktiga eller ofullständiga rättas – vad som kallas kravet på korrekthet – som i dataskyddsförordningen motsvaras av artikel 5.1 d.

Nuvarande bestämmelser i registerförfattningar som utgör undantag från de rättigheter och skyldigheter som föreskrivs i PUL, däribland rätten till rättelse, har ofta sin grund i artikel 13.1 i dataskyddsdirektivet (SOU 2017:39 s. 201). I dataskyddsförordningen finns motsvarigheten till den artikeln i artikel 23, se nedan.

Rättelse enligt personuppgiftslagen

Enligt 28 § PUL är den personuppgiftsansvarige skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med PUL eller föreskrifter som har utfärdats med stöd av PUL. Rubriken närmast före paragrafen lyder ”Rättelse”. Med detta menas rättelse i den vidare bemärkelsen korrigering, som alltså kan ske genom de alternativa metoderna rättelse, blockering och utplåning. Det är den som ska göra korrigeringen, dvs. den personuppgiftsansvarige, som ska välja mellan alternativen (se prop. 1997/98:44 s. 86). Av någon annan lag, eller av sakens natur, kan det dock följa att vissa korrigeringsmetoder inte kan användas i vissa fall, t.ex. när det gäller korrigering av personuppgifter i bokföring. En myndighet får inte heller utplåna uppgifter i en allmän handling, om det skulle strida mot andra bestämmelser. Av 28 § PUL framgår därutöver att den personuppgiftsansvarige i vissa fall ska underrätta en tredje man, till vilken uppgifterna har lämnats ut, om korrigeringsåtgärden.

Paragrafen gäller bara när personuppgifter har behandlats i strid med PUL (eller föreskrifter som utfärdats med stöd av PUL). Detta innebär bl.a. att korrigering enligt 28 § PUL inte kan ske vid överträdelser av sektorsspecifika bestämmelser om personuppgiftsbehandling. I den mån de sektorsspecifika bestämmelserna reglerar frågan om rättelse innehåller de därför särskilda bestämmelser om rättelse eller hänvisningar till andra bestämmelser om rättelse.

Hänvisningar till personuppgiftslagen

På finansmarknadsområdet finns det flera författningar som hänvisar till PUL:s bestämmelser om rättelse. Sådana hänvisningar finns t.ex. i 6 kap. 8 § lagen (2010:751) om betaltjänster och i 8 § förordningen om inlåningsverksamhet.

Hänvisningar till förvaltningslagen

Det finns också flera författningar i vilka det anges att 26 § förvaltningslagen (1986:223) ska tillämpas i stället för 28 § PUL.

Sådan bestämmelse finns i t.ex. 4 kap. 8 § förordningen om bank- och finansieringsrörelse.

Enligt 26 § förvaltningslagen får ett beslut, som innehåller en uppenbar oriktighet till följd av någons skrivfel, räknefel eller liknande förbiseende, rättas av den myndighet som har meddelat beslutet. Innan rättelse sker ska myndigheten ge den som är part tillfälle att yttra sig, om ärendet avser myndighetsutövning mot någon enskild och det inte är obehövligt.

Övriga bestämmelser om rättelse

I kontoföringslagen finns en särskild bestämmelse om rättelse, enligt vilken en registrering ska rättas, om den innehåller någon uppenbar oriktighet till följd av att den som vidtagit registreringsåtgärden eller någon annan har gjort sig skyldig till skrivfel, räknefel eller liknande förbiseende eller till följd av något tekniskt fel (5 kap. 4 §). Den vars rätt berörs ska ges möjlighet att yttra sig, om inte rättelsen är till förmån för denne eller yttrande annars är uppenbart obehövligt.

I ett par andra författningar erinras om att beslut om rättelse får överklagas (9 § förordningen om inlåningsverksamhet och 8 § förordningen om valutaväxling och annan finansiell verksamhet). När det gäller dessa bestämmelser om överklagande, se avsnitt 9.4.

7.4.2 Rättelse enligt dataskyddsförordningen

Enligt artikel 16 i dataskyddsförordningen har den registrerade rätt att utan onödigt dröjsmål få felaktiga personuppgifter rättade av den personuppgiftsansvarige. Med beaktande av ändamålet med behandlingen, ska den registrerade vidare ha rätt att komplettera ofullständiga personuppgifter, bl.a. genom att tillhandahålla ett kompletterande utlåtande.

Av artikel 23 i dataskyddsförordningen följer att rätten till rättelse kan begränsas i unionsrätten eller medlemsstaternas nationella rätt, om en sådan begränsning sker med respekt för andemeningen i de grundläggande fri- och rättigheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att säkerställa vissa i artikeln angivna syften. Ett sådant syfte är andra av unionens eller en medlemsstats viktiga mål av generellt

allmänt intresse (artikel 23.1 e). Ett annat är skydd av den registrerade eller andras rättigheter och friheter (artikel 23.1 i). Sådana begränsande lagstiftningsåtgärder ska emellertid åtminstone, när så är relevant, uppfylla vissa krav, som anges i artikel 23.2.

7.4.3 Anpassningar av bestämmelser om rättelse

Promemorians bedömning: Bestämmelser som innebär att bestämmelsen om rättelse i 26 § förvaltningslagen ska tillämpas bör behållas. Även den särskilda bestämmelsen om rättelse i kontoföringslagen bör behållas.

Promemorians förslag: Hänvisningar i bestämmelser på finansmarknadsområdet till personuppgiftslagens bestämmelser om rättelse ska tas bort. I bestämmelser som anger att rättelsebestämmelsen i 26 § förvaltningslagen ska tillämpas ska hänvisning ske till dataskyddsförordningen i stället för personuppgiftslagen.

Skälen för promemorians förslag och bedömning

Hänvisningar till personuppgiftslagen bör tas bort

De bestämmelser i vilka det anges att PUL:s bestämmelser om rättelse ska tillämpas vid behandling av personuppgifter enligt författningen i fråga måste ändras, eftersom PUL kommer att upphävas. Hänvisningen till PUL har varit nödvändig för att rättelseregeln ska kunna tillämpas i de fall personuppgiftsbehandlingen skett enligt sektorsspecifika bestämmelser. Någon hänvisning till dataskyddsförordningen är inte i något fall nödvändig, eftersom dataskyddsförordningen är direkt tillämplig. Det är därför tillräckligt att hänvisningarna till PUL:s bestämmelser om rättelse tas bort.

Bestämmelser som innebär att bestämmelserna om rättelse i 26 § förvaltningslagen ska tillämpas bör behållas

För rättelse enligt 26 § förvaltningslagen krävs det dels att oriktigheten är uppenbar, dels att oriktigheten beror på skrivfel, räknefel eller liknande förbiseende.

Att den oriktiga uppgiften ska vara uppenbar och bero på vissa angivna förhållanden utgör en begränsning i förhållande till regleringen i artikel 16 i dataskyddsförordningen. En sådan begränsning i vissa register med viktiga rättsverkningar har ansetts förenlig med dataskyddsdirektivet. De register på finansmarknadsområdet där en sådan begränsning av rätten till rättelse gäller utgörs av försäkringsregistret, försäkringsförmedlarregistret, bankregistret, registret över anknutna ombud enligt förordningen om värdepappersmarknaden och registret över personer som har gjort anmälan enligt penningtvättslagen. Med hänsyn till de rättsverkningar som kan vara förenade med införandet i dessa register och mot bakgrund av att möjligheten till undantag från den registrerades rätt till rättelse inte minskats i dataskyddsförordningen jämfört med dataskyddsdirektivet (jfr SOU 2017:39 s. 201–208) bedöms undantagen från rätten till rättelse i dessa bestämmelser vara förenliga med kraven i artikel 23.1 (jfr dock Ds 2017:19 s. 140 f.).

Innan rättelse görs enligt förvaltningslagen ska kommunicering ske, om det är behövligt. Detta bedöms förenligt med dataskyddsförordningen, som har utgångspunkten att rättelse ska ske utan onödigt dröjsmål.

När rätten till rättelse begränsas i nationell rätt måste lagstiftningen åtminstone, när så är relevant, överensstämma med kraven i artikel 23.2 i dataskyddsförordningen. De nu aktuella författningarna bedöms redan förenliga med dessa krav.

Att behålla befintliga bestämmelser som innebär att 26 § förvaltningslagen ska tillämpas är sammanfattningsvis förenligt med dataskyddsförordningen. Hänvisningarna i dessa bestämmelser till 28 § PUL ska dock ändras till hänvisning till artikel 16 i dataskyddsförordningen.

Bestämmelsen i kontoföringslagen om rätten till rättelse bör behållas

Bestämmelserna i dataskyddsförordningen om rättelse motiveras av integritetsskäl. Bestämmelserna om registreringsåtgärder i kontoföringslagen, inbegripet bestämmelsen om rättelse i 5 kap. 4 §, har överförts i stort sett oförändrade från den numera upphävda aktiekontolagen (1989:827) och torde ha utformats efter mönster från annan lagstiftning (t.ex. reglerna om fastighetsregister). Syftet med den typen av särskilda rättelsebestämmelser är primärt att skydda ekonomiska intressen (jfr prop. 1999/2000:39 s. 119 f.).

Rättelse enligt kontoföringslagen förutsätter att oriktigheten är uppenbar till följd av att den som vidtagit registreringsåtgärden eller någon annan har gjort sig skyldig till skrivfel, räknefel eller liknande förbiseende eller till följd av något tekniskt fel. Av samma skäl som anförs ovan när det gäller att behålla hänvisningar till bestämmelsen om rättelse i 26 § förvaltningslagen bör den särskilda bestämmelsen om rättelse i kontoföringslagen behållas.

Vidare förutsätter bestämmelsen i kontoföringslagen som utgångspunkt att kommunikation sker inför rättelsen, medan dataskyddsförordningen kräver att rättelse sker utan onödigt dröjsmål. Med hänsyn till att införande i det nu aktuella registret är förenat med rättsverkningar, bedöms att kommunikation som föregår rättelsen enligt bestämmelsen medför ett nödvändigt dröjsmål. Bestämmelsen om kommunikation bedöms därför förenlig med dataskyddsförordningen.

När rätten till rättelse begränsas i nationell rätt måste lagstiftningen överensstämma med kraven i artikel 23.2 i dataskyddsförordningen. Kontoföringslagen bedöms vara förenlig med dessa krav.

Rätten till komplettering omfattas av rätten till rättelse

Rätten till rättelse enligt dataskyddsförordningen omfattar även rätten till komplettering av ofullständiga uppgifter. Komplettering av ofullständiga uppgifter enligt ovan nämnda författningar på finansmarknadsområdet med särskilda rättelsebestämmelser får anses kunna ske under samma förutsättningar som rättelse av direkta felaktigheter, dvs. i den mån ofullständigheten är uppenbar och beror på förbiseende (jfr JO 1990/91 s. 135). Rätten till

komplettering enligt artikel 16 i dataskyddsförordningen föranleder därför inte några särskilda författningsändringar.

7.5 Rätten till radering

Promemorians bedömning: Rätten till radering enligt dataskyddsförordningen föranleder inte några författningsändringar på finansmarknadsområdet.

Skälen för promemorians bedömning: Rätten till radering eller, som den också kallas, rätten att bli bortglömd, finns i artikel 17 i dataskyddsförordningen. Den ersätter rätten till utplåning i artikel 12 b i dataskyddsdirektivet, som i svensk rätt har genomförts genom 28 § PUL, tillsammans med rätten till rättelse och blockering (se avsnitt 7.4.1). Rätten till utplåning finns inte uttryckligen i de författningar på finansmarknadsområdet enligt vilka bestämmelserna om rättelse i förvaltningslagen eller särskilda bestämmelser om rättelse gäller i stället för 28 § PUL.

Artikel 17 i dataskyddsförordningen är, liksom övriga artiklar i förordningen som behandlar den registrerades rättigheter, direkt tillämplig. Rätten till radering enligt artikeln kommer emellertid att få mycket begränsad betydelse för den personuppgiftsbehandling som sker inom finansmarknadsområdet. Enligt artikel 17.3 b i dataskyddsförordningen gäller nämligen inte rätten till radering om behandling av de aktuella personuppgifterna är nödvändig för att uppfylla en rättslig förpliktelse som kräver behandling enligt unionsrätten eller enligt en medlemsstats nationella rätt, utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning. Så är det regelmässigt för personuppgiftsbehandling som sker med stöd av författningar på finansmarknadsområdet, eftersom den behandlingen sker med stöd av artikel 6.1 c eller e i dataskyddsförordningen (se avsnitt 5.1).

Sammanfattningsvis föranleder rätten till radering enligt artikel 17 i dataskyddsförordningen därför inte några författningsändringar på finansmarknadsområdet.

7.6 Rätten till begränsning av behandling

Promemorians bedömning: Rätten till begränsning av behandling enligt dataskyddsförordningen föranleder inte några författningsändringar på finansmarknadsområdet.

Skälen för promemorians bedömning: Enligt artikel 18 i dataskyddsförordningen har den registrerade rätt att under vissa förutsättningar kräva att behandlingen av personuppgifter begränsas. Med begränsning avses dels åtgärd i form av markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden (artikel 4.3 i förordningen), dels, när det gäller denna framtida hantering, att sådana personuppgifter med undantag för lagring, endast behandlas med den registrerades samtycke eller för att fastställa, göra gällande eller försvara rättsliga anspråk eller för att skydda någon annan fysisk eller juridisk persons rättigheter eller för skäl som rör ett viktigt allmänintresse för unionen eller för en medlemsstat (artikel 18.2).

Rätten till begränsning ersätter den åtgärd som i artikel 12 b i dataskyddsdirektivet benämns som blockering och som i svensk rätt har genomförts genom 28 § PUL, tillsammans med rätten till rättelse och radering (se avsnitt 6.4.1).

Rätten till blockering finns inte uttryckligen i de författningar på finansmarknadsområdet enligt vilka bestämmelserna om rättelse i förvaltningslagen eller särskilda bestämmelser om rättelse gäller i stället för 28 § PUL.

Artikel 18 i dataskyddsförordningen är, liksom övriga artiklar i förordningen som behandlar den registrerades rättigheter, direkt tillämplig. Det saknas anledning att införa en mer långtgående rätt till begränsning än den som krävs enligt dataskyddsförordningen. I de författningar på finansmarknadsområdet som med hänsyn till vissa registers vikt innehåller inskränkningar av rätten till rättelse som gäller enligt artikel 16 i förordningen, finns inte behov av att inskränka rätten till begränsning. I de fall en begränsning av behandlingen skulle inkräkta på någon fysisk eller juridisk persons rättigheter eller något viktigt allmänintresse ska sådan begränsning enligt artikel 18.2 i förordningen nämligen inte ske. De beaktansvärda intressen som kan finnas emot begränsning i nämnda register på finansmarknadsområdet är därmed tillgodosedda genom denna

direkt tillämpliga regel i dataskyddsförordningen (jfr dock Ds 2017:19 s. 146 f.). Rätten till begränsning enligt artikel 18 i förordningen föranleder därför inte några författningsändringar på detta område.

7.7 Rätten till dataportabilitet

Promemorians bedömning: Rätten till dataportabilitet enligt dataskyddsförordningen föranleder inte några författningsändringar på finansmarknadsområdet.

Skälen för promemorians bedömning: Dataportabilitet innebär att uppgifter flyttas från ett nätverk till ett annat. Den registrerade har rätt till dataportabilitet enligt artikel 20 i dataskyddsförordningen. Rätten förutsätter att behandlingen grundar sig på samtycke eller avtal. Personuppgiftsbehandling som regleras i författningarna på finansmarknadsområdet sker emellertid regelmässigt på andra rättsliga grunder (se avsnitt 4.1). Rätten till dataportabilitet enligt artikel 20 i förordningen föranleder därför inte några författningsändringar på detta område. Det ska ändå påpekas att artikeln är direkt tillämplig och kan få betydelse när personuppgiftsbehandlingen sker med stöd av samtycke eller avtal.

7.8 Rätten till invändningar

Promemorians bedömning: Rätten till invändningar enligt dataskyddsförordningen föranleder inte några författningsändringar på finansmarknadsområdet.

Skälen för promemorians bedömning

Dataskyddsdirektivet och personuppgiftslagen

Rätten till invändningar regleras i artikel 14 i dataskyddsdirektivet och har i svensk rätt genomförts genom 11 och 12 §§ PUL.

Enligt 11 § PUL får personuppgifter inte behandlas för ändamål som rör direkt marknadsföring, om den registrerade hos den

personuppgiftsansvarige skriftligen har anmält att han eller hon motsätter sig sådan behandling.

Enligt 12 § PUL har den registrerade vidare rätt att när som helst återkalla sitt samtycke till personuppgiftsbehandlingen. Ytterligare personuppgifter får därefter inte behandlas, om samtycket är en nödvändig förutsättning för behandlingen. Rätten gäller dock endast samtycke enligt 10 § (samtycke för att behandlingen överhuvudtaget ska vara tillåten), enligt 15 § (samtycke till behandling av känsliga personuppgifter) och enligt 34 § (samtycke till överföring av personuppgifter till tredjeland). Fortsatt behandling av redan insamlade personuppgifter får dessutom ske under förutsättning att övriga krav på behandlingen följs.

Av 12 § andra stycket PUL följer att en registrerad, utöver det som följer av 12 § första stycket och 11 §, inte har rätt att motsätta sig sådan behandling av personuppgifter som är tillåten enligt PUL.

Möjligheterna för den registrerade att motsätta sig behandling är alltså begränsade enligt PUL.

Dataskyddsförordningen

Enligt artikel 21 i dataskyddsförordningen har den registrerade rätt att, under vissa förutsättningar, invända mot den personuppgiftsansvariges behandling av personuppgifter.

För personuppgifter som behandlas för att utföra en uppgift av allmänt intresse, som ett led i myndighetsutövning eller efter en intresseavvägning (dvs. behandling enligt artikel 6.1 första stycket e eller f i dataskyddsförordningen) får en invändning göras när som helst. Görs en invändning, får den personuppgiftsansvarige fortsätta att behandla personuppgifterna bara om han eller hon kan påvisa ”tvingande berättigade skäl (”compelling legitimate grounds” i den engelska språkversionen) som väger tyngre än den registrerades intressen, rättigheter och friheter, eller om behandlingen sker för fastställande, utövande eller försvar av rättsliga anspråk.

För personuppgifter som behandlas för direkt marknadsföring får en invändning också göras när som helst. Görs en invändning, får personuppgifterna inte längre behandlas för sådana ändamål. Någon intresseavvägning ska alltså inte göras i de fallen.

För personuppgifter som behandlas för vetenskapliga och historiska forskningsändamål eller statistiska ändamål gäller rätten till invändningar, om behandlingen inte är nödvändig för att utföra en uppgift av allmänt intresse.

Artikel 21 i dataskyddsförordningen är direkt tillämplig men tillämpningsområdet kan begränsas i enlighet med artikel 23.

Överväganden för finansmarknadsområdet

På finansmarknadsområdet finns ett flertal register som förs av hänsyn till viktiga allmänintressen. För att dessa register ska kunna fortsätta att föras och fylla sina syften kan rätten till invändningar inte gälla för dem. Eftersom de registerförande aktörerna är skyldiga att föra dessa register och förteckningar, vilka ska ha ett visst innehåll, utför de nödvändig personuppgiftsbehandling för att fullgöra en rättslig förpliktelse. Det rör sig alltså om behandling enligt artikel 6.1 första stycket c i dataskyddsförordningen. I de fallen gäller inte rätten till invändningar. Artikel 21 i dataskyddsförordningen föranleder därför inte några författningsändringar på finansmarknadsområdet.

7.9 Rätten att motsätta sig automatiserat individuellt beslutsfattande

Promemorians bedömning: Rätten att motsätta sig automatiskt individuellt beslutsfattande enligt dataskyddsförordningen föranleder inte några författningsändringar på finansmarknadsområdet.

Skälen för promemorians bedömning: Enligt artikel 22 i dataskyddsförordningen har den registrerade i vissa fall en rätt att motsätta sig beslut som grundas enbart på automatiserad behandling, inbegripet profilering, om beslutet har rättsliga följder för den registrerade eller på liknande sätt i betydande grad påverkar denne. Det är fråga om att den enskilde inte ska behöva tåla att sådana viktiga beslut fattas utan mänsklig inblandning. Med profilering avses automatisk behandling av personuppgifter för att bedöma

vissa personliga egenskaper hos en fysisk person (artikel 4.4 i dataskyddsförordningen).

Rätten att motsätta sig automatiskt individuellt beslutsfattande finns även i artikel 15 i dataskyddsdirektivet, som i svensk rätt har genomförts genom 29 § PUL.

Några särregler i förhållande till 29 § PUL finns inte på finansmarknadsområdet. Rätten att motsätta sig automatiskt individuellt beslutsfattande enligt artikel 22 i dataskyddsförordningen föranleder därför inte några författningsändringar på finansmarknadsområdet.

8 Rättsmedel, ansvar och sanktioner

8.1 Dataskyddsförordningens bestämmelser

I dataskyddsförordningens kapitel VIII finns bestämmelser om rättsmedel, ansvar och sanktioner. Där behandlas bl.a. den registrerades rätt att lämna in klagomål till tillsynsmyndigheten (artikel 77) och rätten till ett effektivt rättsmedel mot tillsynsmyndighetens beslut (artikel 78) och mot personuppgiftsansvariga och personuppgiftsbiträden (artikel 79). Där finns också bestämmelser om den registrerades rätt till ersättning vid överträdelser av förordningen (artikel 82). Vidare finns bestämmelser av mer processuell karaktär, t.ex. om när ett förfarande ska vilandeförklaras (artikel 81), och bestämmelser om vilka befogenheter som tillsynsmyndigheterna ska ha (artikel 58). Dataskyddsutredningen föreslår hur frågor om sanktioner och processuella frågor ska tas om hand i den svenska lagstiftningen (SOU 2017:39 s. 273–337). Dataskyddsutrednigen föreslår även en upplysningsbestämmelse avseende att dataskyddsförordningens bestämmelser om ersättning är gällande även vid överträdelser av författningar som kompletterar dataskyddsförordningen, se nedan.

8.2 Skadestånd

8.2.1 Gällande rätt

Skadestånd enligt personuppgiftslagen

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 PUL har orsakat.

Ersättningsskyldigheten kan jämkas, om den personuppgiftsansvarige visar att felet inte berodde på denne.

Den nämnda paragrafen i PUL är en sådan specialbestämmelse om skadestånd som tar över de allmänna skadeståndsreglerna i skadeståndslagen (1972:207). I den utsträckning en ersättningsfråga inte berörs i PUL, t.ex. frågan om hur ersättning ska beräknas eller frågan om ansvaret när det finns flera skadeståndsskyldiga, tillämpas däremot allmänna skadeståndsrättsliga regler.

Paragrafen gäller bara skadestånd vid behandling av personuppgifter i strid med PUL. Det innebär bl.a. att skadestånd inte kan utgå enligt PUL vid brott mot sektorsspecifika bestämmelser om behandling av personuppgifter. I flera sektorsspecifika författningar om behandling av personuppgifter regleras därför frågan om skadestånd särskilt eller så finns det hänvisningar till att bestämmelserna om skadestånd i PUL ska gälla även enligt den författningen.

Hänvisningar till personuppgiftslagen

På finansmarknadsområdet finns flera författningar i vilka det anges att bestämmelserna om skadestånd i PUL ska tillämpas vid behandling av personuppgifter enligt författningen i fråga, t.ex. 7 kap. 2 § fjärde stycket kontoföringslagen och 6 kap. 8 § lagen om betaltjänster. Kontoföringslagen innehåller därutöver särskilda bestämmelser om skadestånd avseende behandling av andra uppgifter än personuppgifter (7 kap. 2 § första–tredje styckena).

8.2.2 Skadestånd enligt dataskyddsförordningen

Personuppgiftsansvarigas och personuppgiftsbiträdens ansvar samt registrerades rätt till ersättning regleras i artikel 82 i dataskyddsförordningen. Där anges att varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av förordningen ska ha rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den uppkomna skadan. I artikeln anges vidare att varje personuppgiftsansvarig som har medverkat vid behandlingen ska ansvara för skadan, medan personuppgiftsbiträden ska ansvara endast om de inte har fullgjort sina skyldigheter enligt dataskyddsförordningen eller om de agerat utanför

eller i strid med den personuppgiftsansvariges lagenliga anvisningar. Den personuppgiftsansvarige (eller personuppgiftsbiträdet) ska undgå ansvar endast om han eller hon visar att han eller hon inte på något sätt är ansvarig för händelsen som orsakat skadan. Slutligen anges att om det finns flera personuppgiftsansvariga eller personuppgiftsbiträden, ska varje personuppgiftsansvarig och personuppgiftsbiträde ansvara för hela skadan gentemot den registrerade. Den som betalar full ersättning har dock regressrätt gentemot övriga ansvariga.

I skälen till dataskyddsförordningen anges att behandling som strider mot förordningen omfattar även behandling som strider mot bl.a. medlemsstaternas nationella rätt med närmare specifikation av förordningens bestämmelser (skäl 146). I sammanhanget kan nämnas att Dataskyddsutredningen föreslår att det i den nya dataskyddslagen ska anges att rätten till ersättning enligt dataskyddsförordningen gäller även vid överträdelser av bestämmelser i den lagen och andra författningar som kompletterar dataskyddsförordningen (8 kap. 1 § dataskyddslagen).

Någon möjlighet till undantag i nationell rätt från rätten till ersättning finns inte i dataskyddsförordningen. Förordningens bestämmelser måste dock kunna kompletteras av nationell reglering för att en tillämpning av dem ska kunna vara möjlig. I avsaknad av andra skadeståndsregler blir utgångspunkten därför att dataskyddsförordningen kommer att kompletteras av allmänna skadeståndsregler, i den utsträckning som en ersättningsfråga inte berörs i förordningen.

8.2.3 Anpassning av skadeståndsreglerna

Promemorians förslag: Bestämmelser på finansmarknadsområdet med hänvisningar till bestämmelserna om skadestånd i personuppgiftslagen ska tas bort.

Skälen för promemorians förslag

Hänvisningar till bestämmelserna om skadestånd i personuppgiftslagen bör tas bort

Bestämmelser i författningarna på finansmarknadsområdet kan inte längre ange att bestämmelserna om skadestånd i PUL ska tillämpas vid behandling av personuppgifter enligt författningen i fråga, eftersom PUL kommer att upphävas.

Hänvisning till PUL har varit nödvändig för att skadeståndsbestämmelserna i den lagen ska kunna tillämpas, i den mån behandlingen skett i strid med sektorsspecifik författning och inte i strid med PUL. Någon hänvisning till dataskyddsförordningen kommer däremot inte i något fall vara nödvändig för att bestämmelserna om skadestånd i förordningen ska vara tillämpliga. Behandling som strider mot dataskyddsförordningen inbegriper nämligen behandling som strider mot bl.a. medlemsstaternas nationella rätt med närmare specifikation av förordningens bestämmelser. Det är därför tillräckligt att hänvisningarna till bestämmelserna om skadestånd i PUL tas bort i författningarna på finansmarknadsområdet. Det innebär att 7 kap. 2 § fjärde stycket kontoföringslagen tas bort och i övriga fall att bestämmelser med hänvisning till skadeståndsreglerna i PUL upphävs.

9 Övriga frågor

9.1 Hänvisningar till personuppgiftslagen

Promemorians förslag: Hänvisningar till personuppgiftslagen ska tas bort och i vissa fall ersättas av hänvisningar till dataskyddsförordningen.

Skälen för promemorians förslag

Författningar som innehåller hänvisningar till personuppgiftslagen

Eftersom PUL ska upphävas måste hänvisningar till den lagen tas bort eller ersättas. På finansmarknadsområdet finns bestämmelser som innehåller hänvisningar till PUL i följande författningar.

- Lagen (1991:980) om handel med finansiella instrument.
- Lagen (1998:1479) om värdepapperscentraler och kontoföring av finansiella instrument.
- Lagen (1999:889) om registrering av krigsskada på egendom.
- Lagen (2004:46) om värdepappersfonder.
- Lagen (2004:297) om bank- och finansieringsrörelse.
- Lagen (2007:528) om värdepappersmarknaden.
- Lagen (2010:751) om betaltjänster.
- Försäkringsrörelselagen (2010:2043).
- Lagen (2016:1306) med kompletterande bestämmelser till EU:s marknadsmissbruksförordning.

- Lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism.
- Lagen (2017:631) om registrering av verkliga huvudmän.
- Förordningen (2004:329) om bank- och finansieringsrörelse.
- Förordningen (2004:330) om inlåningsverksamhet.
- Förordningen (2004:331) om anmälningsplikt avseende viss finansiell verksamhet.
- Förordningen (2005:411) om försäkringsförmedling.[1]
- Förordningen (2007:572) om värdepappersmarknaden.
- Förordningen (2009:92) om åtgärder mot penningtvätt och finansiering av terrorism.
- Förordningen (2010:1008) om betaltjänster.
- Försäkringsrörelseförordning (2011:257).
- Förordningen (2011:776) om elektroniska pengar.
- Förordningen (2014:397) om viss verksamhet med konsumentkrediter.
- Förordningen (2016:1033) om verksamhet med bostadskrediter.
- Förordningen (2016:1316) med kompletterande bestämmelser till EU:s marknadsmissbrukförordning.
- Förordningen (2017:667) om registrering av verkliga huvudmän.

Hänvisningar till bestämmelserna i PUL om personuppgiftsansvar, känsliga personuppgifter, personuppgifter om lagöverträdelser m.m., rättelse och skadestånd behandlas ovan i tidigare avsnitt i promemorian. I detta avsnitt behandlas övriga hänvisningar till PUL.

[1] Denna förordning föreslås upphävas innan förslagen i denna promemoria kommer att träda i kraft (se Ds 2017:17) och behandlas därför inte i promemorian i övrigt.

Bestämmelser som erinrar om personuppgiftslagen

Bestämmelser som erinrar om att PUL gäller för den aktuella personuppgiftsbehandlingen, ibland med tillägget att detta gäller om inte annat anges, finns i bl.a. 4 kap. 1 § kontoföringslagen, 2 kap. 17 d § lagen om värdepappersfonder, och 6 kap. 2 a § lagen om bank- och finansieringsrörelse.

Dessa bestämmelser bör tas bort. Det är inte nödvändigt att ersätta dem med hänvisningar till dataskyddsförordningen och de bestämmelser i svenska författningar som kompletterar förordningen.

Direkt marknadsföring

Som framgår av avsnitt 7.8 har den registrerade rätt att invända mot behandling av personuppgifter för direkt marknadsföring enligt 11 § PUL och artikel 21 i dataskyddsförordningen.

Hänvisningar till 11 § PUL finns i 4 kap. 3 § 5 förordningen om bank- och finansieringsrörelse och 4 kap. 5 § 5 försäkringsrörelseförordningen. I dessa bestämmelser anges att ett visst register bl.a. har till ändamål att tillhandahålla uppgifter för uttag av urval av personuppgifter för direkt marknadsföring, dock med den begränsning som följer av 11 § PUL. Med andra ord har registret till ändamål att tillhandahålla uppgifter för direkt marknadsföring, om inte den registrerade har motsatt sig eller invänt mot sådan behandling. Bestämmelserna är förenliga med dataskyddsförordningen. Hänvisningarna till 11 § PUL bör dock ersättas med hänvisningar till artikel 21.2 och 21.3 i dataskyddsförordningen.

Rätten till registerutdrag

Som framgår av avsnitt 7.3 regleras rätten till registerutdrag i 26 § PUL och artikel 15 i dataskyddsförordningen.

Utöver de hänvisningar som behandlas i avsnitt 7.3 finns hänvisningar till 26 § PUL i bl.a. 9 § förordningen om inlåningsverksamhet och 4 kap. 9 § förordningen om bank- och finansieringsrörelse. I dessa bestämmelser erinras om att avslag på ansökan om information enligt 26 § PUL får överklagas till allmän förvaltningsdomstol.

Dataskyddsutredningen föreslår att det i den nya dataskyddslagen ska anges att beslut om bl.a. registerutdrag som har meddelats av en myndighet i egenskap av personuppgiftsansvarig får överklagas till allmän förvaltningsdomstol (8 kap. 2 § dataskyddslagen).

Det är inte nödvändigt att i de nu aktuella författningarna på finansmarknadsområdet erinra om att avslag på en ansökan om information får överklagas. Hänvisningarna till PUL i dessa författningar bör därför tas bort.

Överföring av personuppgifter till tredjeland

Enligt PUL gäller som huvudregel ett förbud mot överföring till tredjeland av personuppgifter som är under behandling och mot överföring av personuppgifter för behandling i tredjeland om landet inte har en adekvat nivå för skyddet av personuppgifterna (33 §). I 34 och 35 §§ PUL finns bestämmelser om undantag från detta förbud.

I 2 kap. 12 § lagen om handel med finansiella instrument finns bestämmelser om att i den utsträckning det krävs för offentliggörande av prospekt enligt 2 kap. 28–30 §§ får personuppgifterna i prospektet föras över till en stat utanför EES. Denna bestämmelse innehåller ingen hänvisning till PUL. Den får snarare betraktas som en särreglering i förhållande till PUL, som tydligen ansetts förenlig med reglerna i dataskyddsdirektivet. Enligt undantagsbestämmelser i både dataskyddsdirektivet (artikel 26.1 d) och dataskyddsförordningen (artikel 49.1 d) får överföring av personuppgifter till tredjeland ske om överföringen är nödvändig av viktiga skäl som rör allmänintresset. Såsom konstateras ovan (se avsnitt 5.1) är de uppgifter som myndigheter och privata aktörer har enligt författningar på finansmarknadsområdet eller enligt beslut som har meddelats med stöd av sådana författningar regelmässigt uppgifter av allmänt intresse. Kravet på offentliggörande av prospekt inför emission enligt 2 kap. 28–30 §§ lagen om handel med finansiella instrument tillgodoser ett viktigt allmänt intresse. Mot bakgrund av detta är bedömningen att överföring av personuppgifter till tredjeland enligt 2 kap. 12 § samma lag uppfyller såväl dataskyddsdirektivets som dataskyddsförordningens krav på att utgöra ett

viktigt allmänt intresse (som erkänts i nationell rätt) för vilket medlemsstater får föreskriva undantag i nationell rätt. Bestämmelsen får därför anses vara förenlig med dataskyddsförordningen.

9.2 Personnummer och annat identifieringsnummer

Promemorians bedömning: Dataskyddsförordningens bestämmelser om identifieringsnummer föranleder inte några författningsändringar på finansmarknadsområdet.

Skälen för promemorians bedömning

Personuppgiftslagen

I PUL finns särskilda bestämmelser om när personnummer och samordningsnummer får behandlas (22 §). Dessa innebär att uppgifter om personnummer eller samordningsnummer får behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Dessa bestämmelser i PUL har införts med anledning av artikel 8.7 i dataskyddsdirektivet, som föreskriver att medlemsstaterna ska bestämma på vilka villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas.

Dataskyddsförordningen

Personnummer och samordningsnummer anses inte som känsliga personuppgifter i dataskyddsförordningens mening, men har ändå en särställning genom att medlemsstaterna ges möjlighet att införa särskilda villkor för behandlingen (artikel 87). Dataskyddsförordningen ställer alltså inte upp något krav på reglering i detta avseende, men av förordningen följer att om medlemsstaterna bestämmer särskilda villkor för sådan behandling, måste lämpliga skyddsåtgärder för de registrerades fri- och rättigheter enligt förordningen säkerställas. Något uttryckligt sådant krav finns inte i

dataskyddsdirektivet. I skälen till dataskyddsförordningen anges det inte heller något som konkretiserar vilken typ av skyddsåtgärder det bör vara frågan om. I denna del finns alltså utrymme för medlemsstaterna att själva bedöma vilka skyddsåtgärder som kan uppfylla kraven i förordningen.

Dataskyddsutredningen

Dataskyddsutredningen bedömer att en särreglering av personnummer och samordningsnummer i den nya dataskyddslagen är motiverad (SOU 2017:39 s. 199 f.). Utredningen konstaterar att det i lagstiftningsärenden under de senaste åren bedömts att den intresseavvägning som i dag sker enligt PUL är flexibel och väl avpassad för att förhindra omotiverad behandling av personnummer och samordningsnummer. Utredningen föreslår mot denna bakgrund en bestämmelse i den nya lagen som motsvarar 22 § (3 kap. 13 § dataskyddslagen). Samtidigt föreslår utredningen att regeringen ska få meddela föreskrifter om i vilka fall behandling av personnummer och samordningsnummer är tillåten (3 kap. 14 § dataskyddslagen).

Bestämmelser om personnummer på finansmarknadsområdet

I författningarna på finansmarknadsområdet finns flera bestämmelser om behandling av personnummer eller annat identifieringsnummer. Dessa avser behandling som är klart motiverad med hänsyn till vikten av en säker identifiering i enlighet med PUL. Som exempel kan nämnas krav på att ett avstämningskonto för förvaltarregistrerade finansiella instrument i förekommande fall ska innehålla annat identifieringsnummer för förvaltaren än organisationsnummer (3 kap. 9 § kontoföringslagen) och krav på att avstämningskonton som läggs upp för ägare av finansiella instrument ska innehålla kontohavarens personnummer (4 kap. 17 § 1 samma lag). Vidare kan nämnas krav på att register över betalningsinstituts och betaltjänstleverantörers ombud ska innehålla dessas personnummer eller motsvarande när det gäller fysiska personer (3 kap. 17 § och 8 kap. 5 § lagen om betaltjänster). Eftersom dessa bestämmelser är förenliga med PUL, är de förenliga

med den föreslagna nya dataskyddslagen och med dataskyddsförordningen.

9.3 Lagring, gallring och arkivering

Promemorians bedömning: I fråga om lagring, gallring och arkivering föranleder dataskyddsförordningen inte några författningsändringar på finansmarknadsområdet.

Skälen för promemorians bedömning: Som framgår av avsnitt 5.1 gäller principen om lagringsminimering vid all personuppgiftsbehandling (artikel 5.1 e dataskyddsförordningen). Principen innebär att personuppgifter som huvudregel inte får förvaras i en form som möjliggör identifiering av den registrerade under längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Samma princip gäller enligt artikel 6.1 e i dataskyddsdirektivet. Huvudregeln har alltså inte ändrats. Vidare tillåter såväl dataskyddsförordningen som dataskyddsdirektivet att avsteg från denna huvudregel görs under vissa förutsättningar. För dataskyddsförordningens del gäller undantaget bl.a. personuppgifter som behandlas enbart för arkivändamål av allmänt intresse. Vidare gäller enligt dataskyddsförordningen att nationella bestämmelser om bl.a. lagringstid är tillåtna enligt artikel 6.3, när behandlingen grundar sig på en rättslig förpliktelse, en arbetsuppgift av allmänt intresse eller myndighetsutövning.

Dataskyddsutredningen bedömer att den behandling av personuppgifter som myndigheter och andra organ utför när de som en följd av bestämmelserna i arkivlagen (1990:782) arkiverar sina allmänna handlingar utgör en vidarebehandling som sker för arkivändamål av allmänt intresse. Behandlingen ska därmed enligt artikel 5.1 b i dataskyddsförordningen inte anses som oförenlig med de ursprungliga ändamålen, och det krävs därför inte någon annan separat rättslig grund än den med stöd av vilken insamlingen av personuppgifter medgavs (SOU 2017:39 s. 216). När det gäller känsliga personuppgifter föreslår utredningen att sådana uppgifter ska få behandlas för arkivändamål av allmänt intresse, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om bevarande och vård av arkiv (3 kap. 6 §

dataskyddslagen). Behandling av personuppgifter som rör fällande domar i brottmål, lagöverträdelser som innefattar brott eller straffprocessuella tvångsmedel föreslås enligt utredningen få ske om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om bevarande och vård av arkiv (3 kap. 11 §).

Utredningen konstaterar att den närmare innebörden av begreppet arkivändamål av allmänt intresse behöver klargöras i rättstillämpningen, men att det i vart fall står klart att den behandling av personuppgifter som sker för att uppfylla krav på bevarande för andra syften, dvs. syften som inte berör många människor på ett bredare plan, inte omfattas av begreppet (samma betänkande s. 214 f.).

På finansmarknadsområdet finns fyra författningar som innehåller bestämmelser som innebär att personuppgifter ska bevaras under viss tid. Dessa finns i 3 kap. 6 c § kontoföringslagen, 10 kap. 2 § lagen om värdepappersmarknaden, 3 kap. 8 § lagen om betaltjänster och 7 § förordningen (2016:69) om värdepapperscentraler och kontoföring av finansiella instrument. Oavsett om den personuppgiftsbehandling som sker i enlighet med dessa författningar omfattas av begreppet arkivändamål av allmänt intresse, eller inte, utgör dessa bestämmelser sådana nationella bestämmelser om lagringstid som är tillåtna enligt artikel 6.3 i dataskyddsförordningen, eftersom behandlingen grundar sig på en rättslig förpliktelse, en uppgift av allmänt intresse eller myndighetsutövning. De bedömningar av vilka lagringstider som är nödvändiga för ändamålet som ligger bakom bestämmelserna är även fortsättningsvis relevanta. Bestämmelserna är därför förenliga med dataskyddsförordningen. Eftersom det inte heller finns något behov av särreglering i förhållande till den föreslagna nya dataskyddslagen, föranleder bestämmelserna i dataskyddsförordningen om lagring, gallring och arkivering inte några författningsändringar på finansmarknadsområdet.

9.4 Bestämmelser om överklagande

Promemorians förslag: Beslut som en myndighet fattar med anledning av att en registrerad utövar sina rättigheter enligt kapitel III i dataskyddsförordningen ska inte omfattas av överklagandeförbudet i förordningen om registrering av verkliga huvudmän. Bestämmelser som erinrar om att vissa beslut enligt personuppgiftslagen får överklagas ska upphävas.

Skälen för promemorians förslag

Överklagandeförbudet i förordningen om registrering av verkliga huvudmän

Enligt förordningen om registrering av verkliga huvudmän får andra beslut än beslut om undantag från kravet på elektronisk anmälan inte överklagas (5 kap. 5 §). Överklagandeförbudet omfattar på så vis bl.a. beslut om rättelse av registrerade personuppgifter.

En registrerad ska enligt dataskyddsförordningen ha rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde (artikel 79). Av sammanhanget framgår att rättsmedlet ska innefatta en rätt att föra talan i domstol. Vilket slags talan som den registrerade ska kunna väcka framgår däremot inte, vare sig av artiklarna i eller av skälen till förordningen.

När den personuppgiftsansvarige är en myndighet kan vissa beslut rörande behandlingen av personuppgifter sägas vara ett utflöde av myndighetens myndighetsutövning (jfr SOU 2017:39 s. 303). Dataskyddsutredningen gör mot denna bakgrund bedömningen att det i den nya dataskyddslagen bör anges en uttrycklig bestämmelse om att vissa myndighetsbeslut får överklagas till allmän förvaltningsdomstol. Rätten att överklaga bör enligt dataskyddsutredningen omfatta beslut som en personuppgiftsansvarig myndighet fattar med anledning av att en registrerad utövar sina rättigheter enligt kapitel III i dataskyddsförordningen. De rättigheter som kan föranleda överklagbara beslut rör information (artikel 12.5), registerutdrag m.m. (artikel 15), rättelse (artikel 16), radering (artikel 17), begränsning

(artikel 18), underrättelse till tredje man om rättelse, radering eller begränsning (artikel 19) och invändningar (artikel 21).

Även om möjlighet till skadeståndstalan på grund av felaktig personuppgiftsbehandling också skulle stå till buds som rättsmedel för en registrerad enligt förordningen om registrering av verkliga huvudmän, så förefaller det inte motiverat att för detta register frångå den princip om rätt till överklagande som dataskyddsutredningen föreslår. Beslut som en myndighet fattar med anledning av att en registrerad utövar sina rättigheter enligt nämnda artiklarn i kapitel III i dataskyddsförordningen bör därför inte omfattas av det aktuella överklagandeförbudet. Ett undantag från överklagandeförbudet avseende sådana beslut ska därför införas i bestämmelsen.

Erinringar om att beslut enligt personuppgiftslagen får överklagas

I två författningar på finansmarknadsområdet erinras om att beslut om rättelse eller om avslag på ansökan om information enligt PUL får överklagas till allmän förvaltningsdomstol enligt 22 a § förvaltningslagen (9 § förordningen om inlåningsverksamhet och 8 § förordningen om valutaväxling och annan finansiell verksamhet). I bägge dessa fall är Finansinspektionen personuppgiftsansvarig för registret i fråga. I ytterligare två författningar erinras på samma sätt om att avslag på ansökan om information enligt PUL får överklagas till allmän förvaltningsdomstol (4 kap. 9 § förordningen om bank- och finansieringsrörelse och 4 kap. 13 § försäkringsrörelseförordningen [2011:257]). I dessa fall är Bolagsverket personuppgiftsansvarig för registret.

Som nämns ovan föreslår Dataskyddsutredningen att det i den nya dataskyddslagen ska anges en uttrycklig bestämmelse om att beslut som en personuppgiftsansvarig myndighet fattar med anledning av att en registrerad utövar sina rättigheter enligt kapitel III i dataskyddsförordningen får överklagas till allmän förvaltningsdomstol. Hänvisningen till PUL och förvaltningslagen blir därmed överspelade. Mot bakgrund av den tydlighet med vilken rätten till överklagande i den föreslagna bestämmelsen i dataskyddslagen kommer att framgå, framstår det inte som behövligt att låta

erinringarna om överklaganderätt i de berörda förordningarna stå kvar. Dessa bestämmelser bör därför upphävas.

10 Ikraftträdande- och övergångsbestämmelser

Promemorians förslag: Författningsändringarna ska träda i kraft den 25 maj 2018.

Promemorians bedömning: Några övergångsbestämmelser behövs inte.

Skälen för promemorians förslag och bedömning: Enligt artikel 99 i dataskyddsförordningen ska förordningen träda i kraft den tjugonde dagen efter det att den har offentliggjorts i Europeiska unionens officiella tidning (vilket var den 24 maj 2016) och börja tillämpas fr.o.m. den 25 maj 2018. Genom de författningsändringar som föreslås i denna promemoria bedöms författningarna på finansmarknadsområdet vara förenliga med förordningens krav. Ändringarna bör träda i kraft samtidigt som dataskyddsförordningen börjar tillämpas, dvs. den 25 maj 2018.

Dataskyddsförordningen möjliggör inte att övergångsbestämmelser införs med innebörden att förordningen inte ska tillämpas efter den 25 maj 2018. Tvärtom är en utgångspunkt att behandling som pågår den dag då förordningen börjar tillämpas fr.o.m. den dagen ska bringas i överensstämmelse med förordningen (skäl 171). Personuppgiftsansvariga och personuppgiftsbiträden får därför förutsättas ha ordnat sin behandling så att exempelvis en begäran om information från en registrerad som inkommit, men inte hunnit besvaras, före den 25 maj 2018 kan tillmötesgås i enlighet med förordningen.

För skadestånd bör äldre bestämmelser gälla, om skadan orsakats före den 25 maj 2018. Att så är fallet följer av allmänna rättsgrundsatser, varför det inte finns något behov av övergångs-

bestämmelser i det avseendet (se prop. 1972:5 s. 593). Inte heller i övrigt finns det skäl att införa övergångsbestämmelser.

Även myndighetsföreskrifter kan behöva ändras eller kompletteras med anledning av dataskyddsförordningen. Sådana ändringar och tillägg bör träda i kraft samtidigt som dataskyddsförordningen börjar tillämpas.

11 Förslagens konsekvenser

Promemorians bedömning: De författningsändringar som föreslås kan medföra marginellt ökade administrativa bördor och därmed kostnader för personuppgiftsansvariga aktörer, främst i anledning av att de registrerades rättigheter stärks. Den eventuella kostnadsökningen för personuppgiftsansvariga myndigheter kan finansieras inom berörda myndigheters nuvarande ramar.

Skälen för promemorians bedömning: I denna promemoria föreslås ändringar i flera författningar på finansmarknadsområdet för att anpassa dem till dataskyddsförordningen. Förslagen kan således sägas utgöra en liten del av ett stort arbete avseende de förändringar som dataskyddsförordningen medför. De viktigaste effekterna av det förändrade dataskyddet beror på regeländringar som ligger utanför denna promemoria och är alltså inte konsekvenser av förslagen i den. De generella anpassningar av svensk rätt som behöver göras i anledning av dataskyddsförordningen föreslås av Dataskyddsutredningen. För en analys av konsekvenserna av utredningens förslag hänvisas till den utredningens betänkande (SOU 2017:39 s. 345–351).

Genom förslagen i denna promemoria bedöms författningarna på finansmarknadsområdet anpassas till dataskyddsförordningens krav. I den bedömningen inbegrips bl.a. att den samlade dataskyddsregleringen är proportionerlig i förhållande till de legitima mål som eftersträvas och att det i vederbörlig utsträckning tas hänsyn till den registrerades rätt till personlig integritet. Några alternativa lösningar synes inte föreligga för anpassningen. De aktörer som kommer att påverkas av förslagen är privatpersoner

och personuppgiftsansvariga myndigheter. Bland myndigheterna berörs främst Finansinspektionen och Bolagsverket.

Förslagen kan komma att medföra marginellt ökade administrativa bördor och därmed kostnader för personuppgiftsansvariga, främst i anledning av att de registrerades rättigheter stärks. Nuvarande rättsläge ändras dock i mycket liten utsträckning, varför den eventuella kostnadsökningen bör kunna finansieras inom t.ex. berörda myndigheters nuvarande ramar.

Förslagen bedöms förbättra skyddet för enskildas personliga integritet, främst i anledning av att de registrerades rättigheter stärks.

Förslagen bedöms inte föranleda negativa effekter för företagens arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt.

Förslagen bedöms inte få några konsekvenser för jämställdheten mellan kvinnor och män.

Förslagen bedöms inte i övrigt ha några sociala eller miljömässiga konsekvenser.

12 Författningskommentar

12.1 Förslaget till lag om ändring i lagen (1991:980) om handel med finansiella instrument

2 kap.

12 §

Paragrafen innehåller bestämmelser om undantag inför upprättandet av ett prospekt och inför offentliggörandet av prospektet enligt 28–30 §§ från förbudet mot att behandla personuppgifter som rör vissa domar och överträdelser m.m.

Ändringen innebär att hänvisningen till 21 § PUL ersätts med en hänvisning till artikel 10 i dataskyddsförordningen.

Övervägandena finns i avsnitt 5.3.

12.2 Förslaget till lag om ändring i lagen (1998:1479) om värdepapperscentraler och kontoföring av finansiella instrument

1 kap.

6 §

Paragrafen behandlar skyldigheten för svenska värdepapperscentraler och kontoförande institut att tillhandahålla ändamålsenliga rapporteringssystem för s.k. visselblåsare.

Ändringen innebär att andra stycket, med erinran om att PUL gäller vid behandling av personuppgifter inom ramen för sådana rapporteringssystem som avses i första stycket, tas bort. Allmänna

bestämmelser om behandling av personuppgifter finns i stället i dataskyddsförordningen.

Övervägandena finns i avsnitt 9.1.

4 kap.

1 §

Paragrafen behandlar hur avstämningsregister ska föras och syftet med registret, samt frågan om personuppgiftsansvar.

I *första stycket* tas hänvisningen till PUL, avseende innebörden av personuppgiftsansvaret, bort. Innebörden av personuppgiftsansvaret kommer i stället att följa av dataskyddsförordningen.

Även *andra stycket* med en erinran om att PUL tillämpas vid behandling av personuppgifter om ägare och innehavare av särskild rätt till finansiella instrument, om inte annat anges, tas bort.

Övervägandena finns i avsnitten 6.3 och 9.1.

7 kap.

2 §

Paragrafen behandlar frågor om skadeståndsansvar vid felaktiga registreringsåtgärder i ett avstämningsregister.

Fjärde stycket, med hänvisning till bestämmelser i PUL om skadestånd, tas bort. Skadestånd vid felaktig personuppgiftsbehandling kommer att regleras av artikel 82 i dataskyddsförordningen. I 8 kap. 1 § i den nya dataskyddslagen finns upplysning om att rätten till ersättning enligt dataskyddsförordningen gäller även vid överträdelser av bestämmelser i den lagen och andra författningar som kompletterar dataskyddsförordningen.

Övervägandena finns i avsnitt 8.2.3.

12.3 Förslaget till lag om ändring i lagen (1999:889) om registrering av krigsskada på egendom

1 §

Paragrafen behandlar hur krigsskaderegistret ska föras och syftet med registret, samt Finansinspektionens personuppgiftsansvar.

Ändringen i *andra stycket* innebär att hänvisningen till PUL, avseende innebörden av personuppgiftsansvaret, tas bort. Innebörden av personuppgiftsansvaret kommer i stället att följa av dataskyddsförordningen.

Övervägandena finns i avsnitt 6.3.

12.4 Förslaget till lag om ändring i lagen (2004:46) om värdepappersfonder

2 kap.

17 d §

Paragrafen behandlar skyldighet för fondbolag att tillhandahålla ändamålsenliga rapporteringssystem för s.k. visselblåsare.

Ändringen innebär att andra stycket, med erinran om att PUL gäller vid behandling av personuppgifter inom ramen för sådana rapporteringssystem som avses i första stycket, tas bort. Allmänna bestämmelser om behandling av personuppgifter finns i stället i dataskyddsförordningen.

Övervägandena finns i avsnitt 9.1.

4 kap.

11 §

Paragrafen behandlar skyldighet för fondbolag att föra eller låta föra register över samtliga innehavare av andelar i fonden.

Ändringen i *första stycket* innebär att erinran om att PUL gäller vid automatiserad och viss manuell behandling av personuppgifter tas bort. Allmänna bestämmelser om behandling av personuppgifter finns i stället i dataskyddsförordningen.

Övervägandena finns i avsnitt 9.1.

12.5 Förslaget till lag om ändring i lagen (2004:297) om bank- och finansieringsrörelse

6 kap.

2 a §

Paragrafen behandlar skyldighet för kreditinstitut att tillhandahålla ändamålsenliga rapporteringssystem för s.k. visselblåsare.

Ändringen innebär att andra stycket, med erinran om att PUL gäller vid behandling av personuppgifter inom ramen för sådana rapporteringssystem som avses i första stycket, tas bort. Allmänna bestämmelser om behandling av personuppgifter finns i stället i dataskyddsförordningen.

Övervägandena finns i avsnitt 9.1.

12.6 Förslaget till lag om ändring i lagen (2007:528) om värdepappersmarknaden

4 kap.

8 §

Paragrafen behandlar skyldighet för företag hemmahörande utanför EES som har fått tillstånd att driva värdepappersrörelse från filial i Sverige att tillhandahålla ändamålsenliga rapporteringssystem för s.k. visselblåsare.

Ändringen innebär att andra stycket, med erinran om att PUL gäller vid behandling av personuppgifter inom ramen för sådana rapporteringssystem som avses i första stycket, tas bort. Allmänna bestämmelser om behandling av personuppgifter finns i stället i dataskyddsförordningen.

Övervägandena finns i avsnitt 9.1.

8 kap.

4 a §

Paragrafen behandlar skyldigheten för ett värdepappersbolag att tillhandahålla ändamålsenliga rapporteringssystem för s.k. visselblåsare.

Ändringen innebär att andra stycket, med erinran om att PUL gäller vid behandling av personuppgifter inom ramen för sådana rapporteringssystem som avses i första stycket, tas bort. Allmänna bestämmelser om behandling av personuppgifter finns i stället i dataskyddsförordningen.

Övervägandena finns i avsnitt 9.1.

10 kap.

15 §

Paragrafen behandlar skyldigheten för den som tillhandahåller en datarapporteringstjänst att ha ändamålsenliga rapporteringssystem för s.k. visselblåsare.

Ändringen innebär att andra stycket, med erinran om att PUL gäller vid behandling av personuppgifter inom ramen för sådana rapporteringssystem som avses i första stycket, tas bort. Allmänna bestämmelser om behandling av personuppgifter finns i stället i dataskyddsförordningen.

Övervägandena finns i avsnitt 9.1.

13 kap.

2 a §

Paragrafen behandlar skyldighet för en börs att tillhandahålla ändamålsenliga rapporteringssystem för s.k. visselblåsare.

Ändringen innebär att andra stycket, med erinran om att PUL gäller vid behandling av personuppgifter inom ramen för sådana rapporteringssystem som avses i första stycket, tas bort. Allmänna

bestämmelser om behandling av personuppgifter finns i stället i dataskyddsförordningen.

Övervägandena finns i avsnitt 9.1.

12.7 Förslaget till lag om ändring i lagen (2010:751) om betaltjänster

6 kap.

1 §

Paragrafen behandlar rätten för en betaltjänstleverantör eller den som ansvarar för ett betalningssystem att behandla personuppgifter och föra register i samband med granskning för att upptäcka misstänkta transaktioner.

Ändringen innebär att erinran om att rätten att behandla personuppgifter och föra register enligt 2–9 §§ gäller utöver PUL tas bort. Allmänna bestämmelser om behandling av personuppgifter finns i dataskyddsförordningen.

Övervägandena finns i avsnitt 9.1.

12.8 Förslaget till lag om ändring i försäkringsrörelselagen (2010:2043)

4 kap.

14 §

Paragrafen stadgar om tystnadsplikt gentemot en förmånstagare avseende behandlad personuppgift som anger att försäkringstagaren har vidtagit dispositioner beträffande försäkringsbelopp som utfaller i framtiden till förmånstagaren.

Ändringen innebär att hänvisningen till PUL ersätts med en hänvisning till dataskyddsförordningen.

Övervägandena finns i avsnitt 7.2.

12.9 Förslaget till lag om ändring i lagen (2016:1306) med kompletterande bestämmelser till EU:s marknadsmissbruksförordning

2 kap.

3 §

Paragrafen behandlar Finansinspektionens skyldighet att föra register över anmälningar som har gjorts enligt artikel 19.1–19.10 i marknadsmissbruksförordningen.

Ändringen i *tredje stycket* innebär att hänvisningen till PUL avseende innebörden av Finansinspektionens personuppgiftsansvar tas bort. Innebörden av personuppgiftsansvaret kommer i stället att följa av dataskyddsförordningen.

Övervägandena finns i avsnitt 6.3.

7 §

Paragrafen behandlar skyldigheten för ett finansiellt företag att tillhandahålla ändamålsenliga rapporteringssystem för s.k. visselblåsare.

Andra stycket första meningen om att PUL gäller vid behandling av personuppgifter inom ramen för sådana rapporteringssystem som avses i första stycket tas bort. Allmänna bestämmelser om behandling av personuppgifter finns i stället i dataskyddsförordningen.

I *andra stycket andra meningen* ersätts hänvisningen till 21 § PUL med en hänvisning till artikel 10 i dataskyddsförordningen.

Övervägandena finns i avsnitten 5.3 och 9.1.

12.10 Förslaget till ändring i lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism

5 kap.

1 §

Paragrafen anger tillämpningsområdet för förevarande kapitel.

Ändringen innebär att andra stycket, med erinran om att PUL gäller vid verksamhetsutövarens behandling av personuppgifter, om inte annat följer av kapitlet, tas bort. Allmänna bestämmelser om behandling av personuppgifter finns i stället i dataskyddsförordningen.

Övervägandena finns i avsnitt 9.1.

5 §

Paragrafen behandlar under vilka förutsättningar en verksamhetsutövare får behandla känsliga personuppgifter.

Ändringen i *första stycket* innebär att hänvisningen till 13 § PUL ersätts med en hänvisning till artikel 9.1 i dataskyddsförordningen. De uppgifter som avses i denna artikel är personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Övervägandena finns i avsnitt 5.2.

6 §

Paragrafen behandlar under vilka förutsättningar personuppgifter om lagöverträdelser får behandlas av en verksamhetsutövare.

Ändringen i *första stycket* innebär att hänvisningen till 13 § PUL ersätts med en hänvisning till artikel 10 i dataskyddsförordningen. De uppgifter som avses i denna artikel är personuppgifter som rör

fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder.

Övervägandena finns i avsnitt 5.2.

6 kap.

4 §

Paragrafen behandlar skyldigheten för verksamhetsutövare att tillhandahålla ändamålsenliga rapporteringssystem för s.k. visselblåsare.

Ändringen innebär att tredje stycket, med erinran om att PUL gäller vid behandling av personuppgifter inom ramen för sådana rapporteringssystem, tas bort. Allmänna bestämmelser om behandling av personuppgifter finns i stället i dataskyddsförordningen.

Övervägandena finns avsnitt 9.1.

12.11 Förslaget till lag om ändring i lagen (2017:631) om registrering av verkliga huvudmän

2 kap.

6 §

Paragrafen behandlar undantag från skyldigheten att anmäla uppgifter om verkliga huvudmän om det medför att känsliga personuppgifter avslöjas.

Ändringen i *andra stycket* innebär att nuvarande hänvisning till uppgift om en fysisk persons medlemskap i fackförening, hälsotillstånd eller sexualliv ersätts med en hänvisning till sådana känsliga personuppgifter som avses i artikel 9.1 i dataskyddsförordningen. På så vis omfattar paragrafen samtliga typer av uppgifter som anges i artikel 9.1, nämligen personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Övervägandena finns i avsnitt 5.2.

I

(Lagstiftningsakter)

FÖRORDNINGAR

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679

av den 27 april 2016

om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 16,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ([1]),

med beaktande av Regionkommitténs yttrande ([2]),

i enlighet med det ordinarie lagstiftningsförfarandet ([3]), och

av följande skäl:

(1) Skyddet för fysiska personer vid behandling av personuppgifter är en grundläggande rättighet. Artikel 8.1 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*) och artikel 16.1 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) föreskriver att var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

(2) Principerna och reglerna för skyddet för fysiska personer vid behandling av deras personuppgifter bör, oavsett deras medborgarskap eller hemvist, respektera deras grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Avsikten med denna förordning är att bidra till att skapa ett område med frihet, säkerhet och rättvisa och en ekonomisk union, till ekonomiska och sociala framsteg, till förstärkning och konvergens av ekonomierna inom den inre marknaden samt till fysiska personers välbefinnande.

(3) Europaparlamentets och rådets direktiv 95/46/EG ([4]) syftar till att harmonisera skyddet av fysiska personers grundläggande rättigheter och friheter vid behandling av personuppgifter och att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna.

([1]) EUT C 229, 31.7.2012, s. 90.
([2]) EUT C 391, 18.12.2012, s. 127.
([3]) Europaparlamentets ståndpunkt av den 12 mars 2014 (ännu ej offentliggjord i EUT) och rådets ståndpunkt vid första behandlingen av den 8 april 2016 (ännu ej offentliggjord i EUT). Europaparlamentets ståndpunkt av den 14 april 2016.
([4]) Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (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 fastställts 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 sektorsspecifika lagar på områden som kräver mer specifika bestämmelser. Denna förordning ger dessutom medlemsstaterna handlingsutrymme att specificera sina bestämmelser, även för behandlingen av särskilda kategorier av personuppgifter (nedan kallade *känsliga uppgifter*). Denna förordning utesluter inte att det i medlemsstaternas nationella rätt fastställs närmare omständigheter för specifika situationer där uppgifter behandlas, inbegripet mer exakta villkor för laglig behandling av personuppgifter.

(11) Ett effektivt skydd av personuppgifter över hela unionen förutsätter att de registrerades rättigheter förstärks och specificeras och att de personuppgiftsansvarigas och personuppgiftsbiträdenas skyldigheter vid behandling av personuppgifter klargörs, samt att det finns likvärdiga befogenheter för övervakning och att det säkerställs att reglerna för skyddet av personuppgifter efterlevs och att sanktionerna för överträdelser är likvärdiga i medlemsstaterna.

(12) I artikel 16.2 i EUF-fördraget bemyndigas Europaparlamentet och rådet att fastställa bestämmelser om skydd för fysiska personer när det gäller behandling av personuppgifter och bestämmelser om den fria rörligheten för personuppgifter.

(13) För att säkerställa en enhetlig nivå för skyddet av fysiska personer över hela unionen och undvika avvikelser som hindrar den fria rörligheten av personuppgifter inom den inre marknaden behövs en förordning som skapar rättslig säkerhet och öppenhet för ekonomiska aktörer, däribland mikroföretag samt små och medelstora företag, och som ger fysiska personer i alla medlemsstater samma rättsligt verkställbara rättigheter och skyldigheter samt ålägger personuppgiftsansvariga och personuppgiftsbiträden samma ansvar, så att övervakningen av behandling av personuppgifter blir enhetlig, sanktionerna i alla medlemsstater likvärdiga och samarbetet mellan tillsynsmyndigheterna i olika medlemsstater effektivt. För att den inre marknaden ska fungera väl krävs att det fria flödet av personuppgifter inom unionen inte begränsas eller förbjuds av skäl som har anknytning till skydd för fysiska personer med avseende på behandling av personuppgifter. För att ta hänsyn till mikroföretagens samt de små och medelstora företagens särskilda situation innehåller denna förordning ett undantag för organisationer som sysselsätter färre än 250 personer med avseende på registerföring. Dessutom uppmanas unionens institutioner och organ samt medlemsstaterna och deras tillsynsmyndigheter att vid tillämpningen av denna förordning ta hänsyn till mikroföretagens samt de små och medelstora företagens särskilda behov. Begreppen mikroföretag samt små och medelstora företag bör bygga på artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG ([1]).

(14) Det skydd som ska tillhandahållas enligt denna förordning bör tillämpas på fysiska personer, oavsett medborgarskap eller hemvist, med avseende på behandling av deras personuppgifter. Denna förordning omfattar inte behandling av personuppgifter rörande juridiska personer, särskilt företag som bildats som juridiska personer, exempelvis uppgifter om namn på och typ av juridisk person samt kontaktuppgifter.

(15) För att förhindra att det uppstår en allvarlig risk för att reglerna kringgås bör skyddet för fysiska personer vara teknikneutralt och inte vara beroende av den teknik som används. Skyddet för fysiska personer bör vara tillämpligt på både automatiserad och manuell behandling av personuppgifter, om personuppgifterna ingår i eller är avsedda att ingå i ett register. Akter eller grupper av akter samt omslag till dessa, som inte är ordnade enligt särskilda kriterier, bör inte omfattas av denna förordning.

(16) Denna förordning är inte tillämplig på frågor som rör skyddet av grundläggande rättigheter och friheter eller det fria flödet av personuppgifter på områden som inte omfattas av unionsrätten, såsom verksamhet rörande nationell säkerhet. Denna förordning är inte tillämplig på medlemsstaternas behandling av personuppgifter när de agerar inom ramen för unionens gemensamma utrikes- och säkerhetspolitik.

(17) Europaparlamentets och rådets förordning (EG) nr 45/2001 ([2]) är tillämplig på den behandling av personuppgifter som sker i unionens institutioner, organ och byråer. Förordning (EG) nr 45/2001 och de av unionens övriga rättsakter som är tillämpliga på sådan behandling av personuppgifter bör anpassas till principerna och bestämmelserna i den här förordningen och tillämpas mot bakgrund av den här förordningen. För att tillhandahålla en stark och sammanhängande ram för dataskyddet inom unionen bör nödvändiga anpassningar av förordning (EG) nr 45/2001 göras när den här förordningen har antagits, så att de båda förordningarna kan tillämpas samtidigt.

(18) Denna förordning är inte tillämplig på fysiska personers behandling av personuppgifter som ett led i verksamhet som är helt och hållet privat eller har samband med personens hushåll och därmed saknar koppling till yrkes- eller affärsmässig verksamhet. Privat verksamhet eller verksamhet som har samband med hushållet kan omfatta

([1]) Kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (K(2003) 1422) (EUT L 124, 20.5.2003, s. 36).

([2]) Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).

korrespondens och innehav av adresser, aktivitet i sociala nätverk och internetverksamhet i samband med sådan verksamhet. Denna förordning är dock tillämplig på personuppgiftsansvariga eller personuppgiftsbiträden som tillhandahåller utrustning för behandling av personuppgifter för sådan privat verksamhet eller hushållsverksamhet.

(19) Skyddet för fysiska personer när det gäller behöriga myndigheters behandling av personuppgifter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten och det fria flödet av sådana uppgifter, säkerställs på unionsnivå av en särskild unionsrättsakt. Därför bör denna förordning inte vara tillämplig på behandling av personuppgifter för dessa ändamål. Personuppgifter som myndigheter behandlar enligt denna förordning och som används för de ändamålen bör emellertid regleras genom en mer specifik unionsrättsakt, nämligen Europaparlamentets och rådets direktiv (EU) 2016/680 ([1]). Medlemsstaterna får anförtro behöriga myndigheter i den mening som avses i direktiv (EU) 2016/680 uppgifter som inte nödvändigtvis utförs för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, så att behandlingen av personuppgifter för dessa andra ändamål, i den mån den omfattas av unionsrätten, omfattas av tillämpningsområdet för denna förordning.

Vad gäller dessa behöriga myndigheters behandling av personuppgifter för ändamål som omfattas av tillämpningsområdet för denna förordning, bör medlemsstaterna kunna bibehålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i denna förordning. I sådana bestämmelser får det fastställas mer specifika krav för dessa behöriga myndigheters behandling av personuppgifter för dessa andra ändamål, med beaktande av respektive medlemsstats konstitutionella, organisatoriska och administrativa struktur. När privata organs behandling av personuppgifter omfattas av tillämpningsområdet för denna förordning, bör denna förordning ge medlemsstaterna möjlighet att, under särskilda villkor, i lag begränsa vissa skyldigheter och rättigheter, om en sådan begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda särskilda viktiga intressen, däribland allmän säkerhet samt förebyggande, förhindrande, utredning, avslöjande och lagföring av brott eller verkställande av straffrättsliga påföljder eller skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten. Detta är exempelvis relevant i samband med bekämpning av penningtvätt eller verksamhet vid kriminaltekniska laboratorier.

(20) Eftersom denna förordning bland annat gäller för verksamhet inom domstolar och andra rättsliga myndigheter, skulle det i unionsrätt eller medlemsstaternas nationella rätt kunna anges vilken behandling och vilka förfaranden för behandling som berörs när det gäller domstolars och andra rättsliga myndigheters behandling av personuppgifter. Tillsynsmyndigheternas behörighet bör inte omfatta domstolars behandling av personuppgifter när detta sker inom ramen för domstolarnas dömande verksamhet, i syfte att säkerställa domstolsväsendets oberoende när det utför sin rättsskipande verksamhet, inbegripet när det fattar beslut. Det bör vara möjligt att anförtro tillsynen över sådan behandling av uppgifter till särskilda organ inom medlemsstaternas rättsväsen, vilka framför allt bör säkerställa efterlevnaden av bestämmelserna i denna förordning, främja domstolsväsendets medvetenhet om sina skyldigheter enligt denna förordning och hantera klagomål relaterade till sådan behandling av uppgifter.

(21) Denna förordning påverkar inte tillämpningen av Europaparlamentets och rådets direktiv 2000/31/EG ([2]), särskilt bestämmelserna om tjänstelevererande mellanhänders 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 informationssamhällets tjänster mellan medlemsstaterna.

(22) All behandling av personuppgifter som sker inom ramen för arbetet på personuppgiftsansvarigas eller personuppgiftsbiträdens verksamhetsställen inom unionen bör ske i överensstämmelse med denna förordning, oavsett om behandlingen i sig äger rum inom unionen. Verksamhetsställe innebär det faktiska och reella utförandet av verksamhet med hjälp av en stabil struktur. Den rättsliga formen för en sådan struktur, oavsett om det är en filial eller ett dotterföretag med status som juridisk person, bör inte vara den avgörande faktorn i detta avseende.

([1]) Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (se sidan 89 i detta nummer av EUT).

([2]) Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (”Direktiv om elektronisk handel”) (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 utbjudande 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 folkrätten, bör denna förordning också vara tillämplig på personuppgiftsansvariga som inte är etablerade inom unionen, exempelvis i en medlemsstats diplomatiska beskickning eller konsulat.

(26) Principerna för dataskyddet bör gälla all information som rör en identifierad eller identifierbar fysisk person. Personuppgifter som har pseudonymiserats och som skulle kunna tillskrivas en fysisk person genom att kompletterande uppgifter används bör anses som uppgifter om en identifierbar fysisk person. För att avgöra om en fysisk person är identifierbar bör man beakta alla hjälpmedel, som t.ex. utgallring, som, antingen av den personuppgiftsansvarige eller av en annan person, rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen. För att fastställa om hjälpmedel med rimlig sannolikhet kan komma att användas för att identifiera den fysiska personen bör man beakta samtliga objektiva faktorer, såsom kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten för behandlingen som den tekniska utvecklingen. Principerna för dataskyddet bör därför inte gälla för anonym information, nämligen information som inte hänför sig till en identifierad eller identifierbar fysisk person, eller för personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte eller inte längre är identifierbar. Denna förordning berör därför inte behandling av sådan anonym information, vilket inbegriper information för statistiska ändamål eller forskningsändamål.

(27) Denna förordning gäller inte behandling av personuppgifter rörande avlidna personer. Medlemsstaterna får fastställa bestämmelser för behandlingen av personuppgifter rörande avlidna personer.

(28) Tillämpningen av pseudonymisering av personuppgifter kan minska riskerna för de registrerade som berörs och hjälpa personuppgiftsansvariga och personuppgiftsbiträden att fullgöra sina skyldigheter i fråga om dataskydd. Ett uttryckligt införande av *pseudonymisering* i denna förordning är inte avsett att utesluta andra åtgärder för dataskydd.

(29) För att skapa incitament för tillämpning av pseudonymisering vid behandling av personuppgifter bör åtgärder för pseudonymisering som samtidigt medger en allmän analys vara möjliga inom samma personuppgiftsansvarigs verksamhet, när den personuppgiftsansvarige har vidtagit de tekniska och organisatoriska åtgärder som är nödvändiga för att se till att denna förordning genomförs för berörd uppgiftsbehandling och att kompletterande uppgifter för tillskrivning av personuppgifterna till en specifik registrerad person förvaras separat. Den personuppgiftsansvarige som behandlar personuppgifterna bör ange behöriga personer inom samma personuppgiftsansvarigs verksamhet.

(30) Fysiska personer kan knytas till nätidentifierare som lämnas av deras utrustning, applikationer, verktyg och protokoll, t.ex. ip-adresser, kakor eller andra identifierare, som radiofrekvensetiketter. Detta kan efterlämna spår som, särskilt i kombination med unika identifierare och andra uppgifter som tas emot av servrarna, kan användas för att skapa profiler för fysiska personer och identifiera dem.

(31) Offentliga myndigheter som för sin myndighetsutövning mottar personuppgifter i enlighet med en rättslig förpliktelse, t.ex. skatte- och tullmyndigheter, finansutredningsgrupper, oberoende administrativa myndigheter eller finansmarknadsmyndigheter med ansvar för reglering och övervakning av värdepappersmarknader, bör inte betraktas som mottagare om de tar emot personuppgifter som är nödvändiga för utförandet av en särskild utredning av allmänt intresse, i enlighet med unionsrätten eller medlemstaternas nationella rätt. Offentliga myndigheters begäranden om att uppgifter ska lämnas ut ska alltid vara skriftliga och motiverade, läggas fram i enskilda fall och inte gälla hela register eller leda till att register kopplas samman. Dessa offentliga myndigheters behandling av personuppgifter bör ske i överensstämmelse med de bestämmelser för dataskydd som är tillämpliga på behandlingens ändamål.

(32) Samtycke bör lämnas genom en entydig bekräftande handling som innebär ett frivilligt, specifikt, informerat och otvetydigt medgivande från den registrerades sida om att denne godkänner behandling av personuppgifter rörande honom eller henne, som t.ex. genom en skriftlig, inklusive elektronisk, eller muntlig förklaring. Detta kan inbegripa att en ruta kryssas i vid besök på en internetsida, genom val av inställningsalternativ för tjänster på informationssamhällets område eller genom någon annan förklaring eller något annat beteende som i sammanhanget tydligt visar att den registrerade godtar den avsedda behandlingen av sina personuppgifter. Tystnad, på förhand ikryssade rutor eller inaktivitet bör därför inte utgöra samtycke. Samtycket bör gälla all behandling som utförs för samma ändamål. Om behandlingen tjänar flera olika syften, bör samtycke ges för samtliga syften. Om den registrerade ska lämna sitt samtycke efter en elektronisk begäran, måste denna vara tydlig och koncis och får inte onödigtvis störa användningen av den tjänst som den avser.

(33) Det är ofta inte möjligt att fullt ut identifiera syftet med en behandling av personuppgifter för vetenskapliga forskningsändamål i samband med insamlingen av uppgifter. Därför bör registrerade kunna ge sitt samtycke till vissa områden för vetenskaplig forskning, när vedertagna etiska standarder för vetenskaplig forskning iakttas. Registrerade bör ha möjlighet att endast lämna sitt samtycke till vissa forskningsområden eller delar av forskningsprojekt i den utsträckning det avsedda syftet medger detta.

(34) Genetiska uppgifter bör definieras som personuppgifter som rör en fysisk persons nedärvda eller förvärvade genetiska kännetecken, vilka framgår av en analys av ett biologiskt prov från den fysiska personen i fråga, framför allt kromosom-, DNA- eller RNA-analys eller av en annan form av analys som gör det möjligt att inhämta motsvarande information.

(35) Personuppgifter om hälsa bör innefatta alla de uppgifter som hänför sig till en registrerad persons hälsotillstånd som ger information om den registrerades tidigare, nuvarande eller framtida fysiska eller psykiska hälsotillstånd. Detta inbegriper uppgifter om den fysiska personen som insamlats i samband med registrering för eller tillhandahållande av hälso- och sjukvårdstjänster till den fysiska personen enligt Europaparlamentets och rådets direktiv 2011/24/EU ([1]), ett nummer, en symbol eller ett kännetecken som den fysiska personen tilldelats för att identifiera denne för hälso- och sjukvårdsändamål, uppgifter som härrör från tester eller undersökning av en kroppsdel eller kroppssubstans, däribland genetiska uppgifter och biologiska prov, och andra uppgifter om exempelvis sjukdom, funktionshinder, sjukdomsrisk, sjukdomshistoria, klinisk behandling eller den registrerades fysiologiska eller biomedicinska tillstånd, oberoende av källan, exempelvis från en läkare eller från annan sjukvårdspersonal, ett sjukhus, en medicinteknisk produkt eller ett diagnostiskt in vitro-test.

(36) Den personuppgiftsansvariges huvudsakliga verksamhetsställe i unionen bör vara den plats i unionen där den personuppgiftsansvarige har sin centrala förvaltning, såvida inte beslut om ändamålen och medlen för behandling av personuppgifter fattas vid ett annat av den personuppgiftsansvariges verksamhetsställen i unionen; i sådant fall

([1]) Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).

bör det andra verksamhetsstället anses vara det huvudsakliga verksamhetsstället. En personuppgiftsansvarigs huvudsakliga verksamhetsställe inom unionen bör avgöras med beaktande av objektiva kriterier och bör inbegripa den faktiska och reella ledning som fattar de huvudsakliga besluten vad avser ändamål och medel för behandlingen med hjälp av en stabil struktur. Detta kriterium bör inte vara avhängigt av om behandlingen av personuppgifter utförs på detta ställe. Att tekniska medel och teknik för behandling av personuppgifter eller behandlingsverksamhet finns och används visar i sig inte att det rör sig om ett huvudsakligt verksamhetsställe och utgör därför inte avgörande kriterier för ett huvudsakligt verksamhetsställe. Personuppgiftsbiträdets 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 företagets huvudsakliga verksamhetsställe betraktas som koncernens huvudsakliga verksamhetsställe, utom då behandlingens ändamål och de medel med vilka den utförs fastställs av ett annat företag.

(37) En koncern bör innefatta ett kontrollerande företag och de företag som detta företag kontrollerar (kontrollerade företag), varvid det kontrollerande företaget bör vara det företag som kan utöva ett dominerande inflytande på de övriga företagen i kraft av exempelvis ägarskap, finansiellt deltagande eller de bestämmelser som det regleras av eller befogenheten att införa regler som rör personuppgiftsskyddet. Ett företag med kontroll över behandlingen av personuppgifter vid företag som är underställda detta företag bör, tillsammans med dessa företag, anses utgöra en koncern.

(38) Barns personuppgifter förtjänar särskilt skydd, eftersom barn kan vara mindre medvetna om berörda risker, följder och skyddsåtgärder samt om sina rättigheter när det gäller behandling av personuppgifter. Sådant särskilt skydd bör i synnerhet gälla användningen av barns personuppgifter i marknadsföringssyfte eller för att skapa personlighets- eller användarprofiler samt insamling av personuppgifter med avseende på barn när tjänster som erbjuds direkt till barn utnyttjas. Samtycke från den person som har föräldraansvar över ett barn bör inte krävas för förebyggande eller rådgivande tjänster som erbjuds direkt till barn.

(39) Varje behandling av personuppgifter måste vara laglig och rättvis. Det bör vara klart och tydligt för fysiska personer hur personuppgifter som rör dem insamlas, används, konsulteras eller på annat sätt behandlas samt i vilken utsträckning personuppgifterna behandlas eller kommer att behandlas. Öppenhetsprincipen kräver att all information och kommunikation i samband med behandlingen av dessa personuppgifter är lättillgänglig och lättbegriplig samt att ett klart och tydligt språk används. Den principen gäller framför allt informationen till registrerade om den personuppgiftsansvariges identitet och syftet med behandlingen samt ytterligare information för att sörja för en rättvis och öppen behandling för berörda fysiska personer och deras rätt att erhålla bekräftelse på och meddelande om vilka personuppgifter rörande dem som behandlas. Fysiska personer bör göras medvetna om risker, regler, skyddsåtgärder och rättigheter i samband med behandlingen av personuppgifter och om hur de kan utöva sina rättigheter med avseende på behandlingen. De specifika ändamål som personuppgifterna behandlas för bör vara tydliga och legitima och ha bestämts vid den tidpunkt då personuppgifterna samlades in. Personuppgifterna bör vara adekvata, relevanta och begränsade till vad som är nödvändigt för de ändamål som de behandlas för. Detta kräver i synnerhet att det tillses att den period under vilken personuppgifterna lagras är begränsad till ett strikt minimum. Personuppgifter bör endast behandlas om syftet med behandlingen inte rimligen kan uppnås genom andra medel. För att säkerställa att personuppgifter inte sparas längre än nödvändigt bör den personuppgiftsansvarige införa tidsfrister för radering eller för regelbunden kontroll. Alla rimliga åtgärder bör vidtas för att rätta eller radera felaktiga uppgifter. Personuppgifter bör behandlas på ett sätt som säkerställer lämplig säkerhet och konfidentialitet för personuppgifterna samt förhindrar obehörigt tillträde till och obehörig användning av personuppgifter och den utrustning som används för behandlingen.

(40) För att behandling ska vara laglig bör personuppgifterna behandlas efter samtycke från den berörda registrerade eller på någon annan legitim grund som fastställts i lag, antingen i denna förordning eller i annan unionsrätt eller

medlemsstaternas nationella rätt enligt denna förordning, vilket inbegriper att de rättsliga skyldigheter som åligger den personuppgiftsansvarige måste fullgöras eller att ett avtal i vilket den registrerade är part måste genomföras eller att åtgärder på begäran av den registrerade måste vidtas innan avtalet ingås.

(41) När det i denna förordning hänvisas till en rättslig grund eller lagstiftningsåtgärd, innebär detta inte nödvändigtvis en lagstiftningsakt antagen av ett parlament, utan att detta påverkar krav som uppställs i den konstitutionella ordningen i den berörda medlemsstaten. En sådan rättslig grund eller lagstiftningsåtgärd bör dock vara tydlig och precis och dess tillämpning bör vara förutsägbar för personer som omfattas av den, i enlighet med rättspraxis vid Europeiska unionens domstol (nedan kallad *domstolen*) och Europeiska domstolen för de mänskliga rättigheterna.

(42) När behandling sker efter samtycke från registrerade, bör personuppgiftsansvariga kunna visa att de registrerade har lämnat sitt samtycke till behandlingen. I synnerhet vid skriftliga förklaringar som rör andra frågor bör det finnas skyddsåtgärder som säkerställer att de registrerade är medvetna om att samtycke ges och om hur långt samtycket sträcker sig. I enlighet med rådets direktiv 93/13/EEG ([1]) bör en förklaring om samtycke som den personuppgiftsansvarige i förväg formulerat tillhandahållas i en begriplig och lätt tillgänglig form, med användning av ett klart och tydligt språk och utan 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 ojämlikhet mellan den registrerade och den personuppgiftsansvarige, särskilt om den personuppgiftsansvarige är en offentlig myndighet och det därför är osannolikt att samtycket har lämnats frivilligt när det gäller alla förhållanden som denna särskilda situation omfattar. Samtycke antas inte vara frivilligt om det inte medger att separata samtycken lämnas för olika behandlingar av personuppgifter, trots att detta är lämpligt i det enskilda fallet, eller om genomförandet av ett avtal – inbegripet tillhandahållandet av en tjänst – är avhängigt av samtycket, trots att samtycket inte är nödvändigt för ett sådant genomförande.

(44) Behandling bör vara laglig när den är nödvändig i samband med avtal eller när det finns en avsikt att ingå ett avtal.

(45) Behandling som grundar sig på en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller behandling som krävs för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning, bör ha en grund i unionsrätten eller i en medlemsstats nationella rätt. Denna förordning medför inte något krav på en särskild lag för varje enskild behandling. Det kan räcka med en lag som grund för flera behandlingar som bygger på en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller om behandlingen krävs för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning. Behandlingens syfte bör också fastställas i unionsrätten eller i medlemsstaternas nationella rätt. Därtill skulle man genom denna grund kunna ange denna förordnings allmänna villkor för laglig personuppgiftsbehandling och precisera kraven för att fastställa vem den personuppgiftsansvarige är, vilken typ av personuppgifter som ska behandlas, vilka registrerade som berörs, de enheter till vilka personuppgifterna får lämnas ut, ändamålsbegränsningar, lagringstid samt andra åtgärder för att tillförsäkra en laglig och rättvis behandling. Unionsrätten eller medlemsstaternas nationella rätt bör också reglera frågan huruvida en personuppgiftsansvarig som utför en uppgift av allmänt intresse eller som ett led i myndighetsutövning ska vara en offentlig myndighet eller någon annan fysisk eller juridisk person som omfattas av offentligrättslig lagstiftning eller, om detta motiveras av allmänintresset, vilket inbegriper hälso- och sjukvårdsändamål, såsom folkhälsa och socialt skydd och förvaltning av hälso- och sjukvårdstjänster, av civilrättslig lagstiftning, exempelvis en yrkesorganisation.

(46) Behandling av personuppgifter bör även anses laglig när den är nödvändig för att skydda ett intresse som är av avgörande betydelse för den registrerades eller en annan fysisk persons liv. Behandling av personuppgifter på

([1]) Rådets direktiv 93/13/EEG av den 5 april 1993 om 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 informationssäkerhet, dvs. förmågan hos ett nät eller ett informationssystem att vid en viss tillförlitlighetsnivå tåla olyckshändelser, olagliga handlingar eller illvilligt uppträdande som äventyrar tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade eller överförda personuppgifter och säkerheten hos besläktade tjänster som tillhandahålls av – eller är tillgängliga via – dessa nät och system, av myndigheter, incidenthanteringsorganisationer (Cert), enheter för hantering av datasäkerhetsincidenter, tillhandahållare av elektroniska kommunikationsnät och kommunikationstjänster och tillhandahållare av säkerhetsteknik och säkerhetstjänster. Detta skulle t.ex. kunna innefatta att förhindra obehörigt tillträde till elektroniska kommunikationsnät och felaktig kodfördelning och att sätta stopp för överbelastningsattacker och skador på datasystem och elektroniska kommunikationssystem.

(50) Behandling av personuppgifter för andra ändamål än de för vilka de ursprungligen samlades in bör endast vara tillåten, när detta är förenligt med de ändamål för vilka personuppgifterna ursprungligen samlades in. I dessa fall krävs det inte någon annan separat rättslig grund än den med stöd av vilken insamlingen av personuppgifter medgavs. Om behandlingen är nödvändig för att fullgöra en uppgift av allmänt intresse eller som ett led i myndighetsutövning som den personuppgiftsansvarige har fått i uppgift att utföra, kan unionsrätten eller medlemsstaternas nationella rätt fastställa och närmare ange för vilka uppgifter och syften ytterligare behandling bör betraktas som förenlig och laglig. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör betraktas som förenlig och laglig behandling av uppgifter. Den rättsliga grund för behandling av personuppgifter som återfinns i unionsrätten eller i medlemsstaternas nationella rätt kan också utgöra en rättslig grund för ytterligare behandling. För att fastställa om ett ändamål med den ytterligare behandlingen är förenligt med det ändamål för vilket personuppgifterna ursprungligen insamlades bör den personuppgiftsansvarige, efter att ha uppfyllt alla krav vad beträffar den ursprungliga behandlingens lagenlighet, bland annat beakta alla kopplingar mellan dessa ändamål och ändamålen med den avsedda ytterligare behandlingen, det sammanhang inom vilket personuppgifterna insamlats, särskilt de registrerades rimliga förväntningar till följd av förhållandet till den personuppgiftsansvarige i fråga om den

art, den planerade ytterligare behandlingens konsekvenser för de registrerade samt förekomsten av lämpliga skyddsåtgärder för både den ursprungliga och den planerade ytterligare behandlingen.

Om den registrerade har gett sitt medgivande eller behandlingen grundar sig på unionsrätten eller på medlemsstaternas nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa i synnerhet viktiga mål av allmänt intresse, bör den personuppgiftsansvarige tillåtas att behandla personuppgifterna ytterligare, oavsett om detta är förenligt med ändamålen eller inte. Under alla omständigheter bör tillämpningen av principerna i denna förordning, särskilt informationen till den registrerade om dessa andra ändamål och om dennes rättigheter, inbegripet rätten att göra invändningar, säkerställas. Om den personuppgiftsansvarige anmäler möjliga brott eller hot mot den allmänna säkerheten och i enskilda fall eller i flera fall som rör samma brott eller hot mot den allmänna säkerheten överför dessa personuppgifter till en behörig myndighet, ska detta betraktas som att den personuppgiftsansvarige agerar i ett berättigat intresse. Sådan överföring i den personuppgiftsansvariges berättigade intresse eller ytterligare behandling av personuppgifter bör emellertid vara förbjuden, om behandlingen inte är förenlig med lagstadgad eller yrkesmässig tystnadsplikt eller annan bindande tystnadsplikt.

(51) Personuppgifter som till sin natur är särskilt känsliga med hänsyn till grundläggande rättigheterna och friheter bör åtnjuta särskilt skydd, eftersom behandling av sådana uppgifter kan innebära betydande risker för de grundläggande rättigheterna och friheterna. Dessa personuppgifter bör även inbegripa personuppgifter som avslöjar ras eller etniskt ursprung, varvid användningen av termen *ras* i denna förordning inte innebär att unionen godtar teorier som söker fastställa förekomsten av skilda människoraser. Behandling av foton bör inte systematiskt anses utgöra behandling av särskilda kategorier av personuppgifter, eftersom foton endast definieras som biometriska uppgifter när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person. Sådana personuppgifter bör inte behandlas, såvida inte behandling medges i särskilda fall som fastställs i denna förordning, med beaktande av att det i medlemsstaternas lagstiftning får införas särskilda bestämmelser om dataskydd för att anpassa tillämpningen av bestämmelserna i denna förordning i syfte att fullgöra en rättslig skyldighet eller en uppgift av allmänt intresse eller som ett led i myndighetsutövning som den personuppgiftsansvarige har fått i uppgift att utföra. Utöver de särskilda kraven för sådan behandling, bör de allmänna principerna och andra bestämmelser i denna förordning tillämpas, särskilt när det gäller villkoren för laglig behandling. Undantag från det allmänna förbudet att behandla sådana särskilda kategorier av personuppgifter bör uttryckligen fastställas, bland annat om den registrerade lämnar sitt uttryckliga samtycke eller för att tillgodose specifika behov, i synnerhet när behandlingen utförs inom ramen för legitima verksamheter som bedrivs av vissa sammanslutningar eller stiftelser i syfte att göra det möjligt att utöva grundläggande friheter.

(52) Undantag från förbudet att behandla särskilda kategorier av personuppgifter bör även tillåtas om de föreskrivs i unionsrätten eller i medlemsstaternas nationella rätt och underkastas lämpliga skyddsåtgärder för att skydda personuppgifter och övriga grundläggande rättigheter, när allmänintresset motiverar detta, i synnerhet i fråga om behandling av personuppgifter inom ramen för arbetsrätt och sociallagstiftning, däribland pensioner, och för hälsosäkerhetsändamål, övervaknings- och varningssyften, förebyggande eller kontroll av smittsamma sjukdomar och andra allvarliga hot mot hälsan. Detta undantag får göras för hälsoändamål, inbegripet folkhälsa och förvaltningen av hälso- och sjukvårdstjänster, särskilt för att säkerställa kvalitet och kostnadseffektivitet i de förfaranden som används vid prövningen av ansökningar om förmåner och tjänster inom sjukförsäkringssystemet, eller för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Genom undantag bör man även tillåta behandling av sådana personuppgifter där så krävs för fastställande, utövande eller försvar av rättsliga anspråk, oavsett om detta sker inom ett domstolsförfarande eller inom ett administrativt eller ett utomrättsligt förfarande.

(53) Särskilda kategorier av personuppgifter som förtjänar ett mer omfattande skydd bör endast behandlas i hälsorelaterade syften om detta krävs för att uppnå dessa syften och gagnar fysiska personer och samhället i stort, särskilt inom ramen för förvaltningen av tjänster för hälso- och sjukvård och social omsorg och deras system, inbegripet behandling som utförs av förvaltningen och centrala nationella hälsovårdsmyndigheter av sådana uppgifter för syften som hör samman med kvalitetskontroll, information om förvaltningen samt allmän nationell och lokal tillsyn över hälso- och sjukvårdssystemet och systemet för social omsorg och säkerställande av kontinuitet inom hälso- och sjukvård och social omsorg samt gränsöverskridande hälso- och sjukvård eller hälsosäkerhet, syften som hör samman med övervakning samt varningssyften eller för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål som baseras på unionsrätten eller på medlemsstaternas nationella rätt, vilka måste ha ett syfte av allmänt intresse, samt studier som genomförs av allmänt intresse på folkhälsoområdet. Denna förordning bör därför innehålla harmoniserade villkor för behandling av särskilda kategorier av personuppgifter om hälsa, vad gäller särskilda behov, i synnerhet när behandlingen av uppgifterna utförs för vissa hälsorelaterade syften av personer som enligt lag är underkastade

yrkesmässig tystnadsplikt. Unionsrätten eller medlemsstaternas nationella rätt bör föreskriva särskilda och lämpliga åtgärder som skyddar fysiska personers grundläggande rättigheter och personuppgifter. Medlemsstaterna bör få behålla eller införa ytterligare villkor, även begränsningar, för behandlingen av genetiska eller biometriska uppgifter eller uppgifter om hälsa. Detta bör emellertid inte hindra det fria flödet av personuppgifter inom unionen, när villkoren tillämpas på gränsöverskridande behandling av sådana uppgifter.

(54) På folkhälsoområdet kan det bli nödvändigt att med hänsyn till ett allmänt intresse behandla särskilda kategorier av personuppgifter utan att den registrerades samtycke inhämtas. Sådan behandling bör förutsätta lämpliga och särskilda åtgärder för att skydda fysiska personers rättigheter och friheter. I detta sammanhang bör *folkhälsa* tolkas enligt definitionen i Europaparlamentets och rådets förordning (EG) nr 1338/2008 ([1]), nämligen alla aspekter som rör hälsosituationen, dvs. allmänhetens hälsotillstånd, inbegripet sjuklighet och funktionshinder, hälsans 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.

([1]) 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 personuppgiftsbehandlingens specifika omständigheter och sammanhang. Dessutom bör den registrerade informeras om förekomsten av profilering samt om konsekvenserna av sådan profilering. Om personuppgifterna samlas in från den registrerade, bör denne även informeras om huruvida han eller hon är skyldig att tillhandahålla personuppgifterna och om konsekvenserna om han eller hon inte lämnar dem. Denna information får tillhandahållas kombinerad med standardiserade symboler för att ge en överskådlig, begriplig, lättläst och meningsfull överblick över den planerade behandlingen. Om sådana symboler visas elektroniskt bör de vara maskinläsbara.

(61) Information om behandling av personuppgifter som rör den registrerade bör lämnas till honom eller henne vid den tidpunkt då personuppgifterna samlas in från den registrerade eller, om personuppgifterna erhålls direkt från en annan källa, inom en rimlig period, beroende på omständigheterna i fallet. Om personuppgifter legitimt kan lämnas ut till en annan mottagare, bör de registrerade informeras första gången personuppgifterna lämnas ut till denna mottagare. Om den personuppgiftsansvarige avser att behandla personuppgifter för ett annat ändamål än det för vilket uppgifterna insamlades, bör denne före ytterligare behandling informera den registrerade om detta andra syfte och lämna annan nödvändig information. Om personuppgifternas ursprung inte kan meddelas den registrerade på grund av att olika källor har använts, bör allmän information ges.

(62) Det är dock inte nödvändigt att införa någon skyldighet att tillhandahålla information, om den registrerade redan innehar denna information, om registreringen eller utlämnandet av personuppgifterna uttryckligen föreskrivs i lag eller om det visar sig vara omöjligt eller skulle medföra orimliga ansträngningar att tillhandahålla den registrerade informationen. Det sistnämnda skulle särskilt kunna vara fallet om behandlingen sker för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. I detta avseende bör antalet registrerade, uppgifternas ålder och lämpliga skyddsåtgärder beaktas.

(63) Den registrerade bör ha rätt att få tillgång till personuppgifter som insamlats om denne samt på enkelt sätt och med rimliga intervall kunna utöva denna rätt, för att vara medveten om att behandling sker och kunna kontrollera att den är laglig. Detta innefattar rätten för registrerade att få tillgång till uppgifter om sin hälsa, exempelvis uppgifter i läkarjournaler med t.ex. diagnoser, undersökningsresultat, bedömningar av behandlande läkare och eventuella vårdbehandlingar eller interventioner. Alla registrerade bör därför ha rätt att få kännedom och underrättelse om framför allt orsaken till att personuppgifterna behandlas, om möjligt vilken tidsperiod behandlingen pågår, vilka som mottar personuppgifterna, bakomliggande logik i samband med automatisk behandling av personuppgifter och, åtminstone när behandlingen bygger på profilering, konsekvenserna av sådan behandling. Om möjligt bör den personuppgiftsansvarige kunna ge fjärråtkomst till ett säkert system genom vilket den registrerade kan få direkt åtkomst till sina personuppgifter. Denna rätt bör inte inverka menligt på andras rättigheter eller friheter, t.ex. affärshemligheter eller immateriell äganderätt och särskilt inte på upphovsrätt som skyddar programvaran. Resultatet av dessa överväganden bör dock inte bli att den registrerade förvägras all information. Om den personuppgiftsansvarige behandlar en stor mängd uppgifter om den registrerade, bör den personuppgiftsansvarige kunna begära att den registrerade lämnar uppgift om vilken information eller vilken behandling en framställan avser, innan informationen lämnas ut.

(64) Personuppgiftsansvariga bör vidta alla rimliga åtgärder för att kontrollera identiteten på en registrerad som begär tillgång, särskilt inom ramen för nättjänster och i fråga om nätidentifierare. Personuppgiftsansvariga bör inte behålla personuppgifter enbart för att kunna agera vid en potentiell begäran.

(65) Den registrerade bör ha rätt att få sina personuppgifter rättade och en *rätt att bli bortglömd*, om lagringen av uppgifterna strider mot denna förordning eller unionsrätten eller medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av. En registrerad bör särskilt ha rätt att få sina personuppgifter raderade och kunna begära att dessa personuppgifter inte behandlas, om de inte längre behövs med tanke på de ändamål för vilka de samlats in eller på annat sätt behandlats, om en registrerad har återtagit sitt samtycke till behandling eller invänder mot behandling av personuppgifter som rör honom eller henne, eller om behandlingen av hans eller

hennes personuppgifter på annat sätt inte överensstämmer med denna förordning. Denna rättighet är särskilt relevant när den registrerade har gett sitt samtycke som barn, utan att vara fullständigt medveten om riskerna med behandlingen, och senare vill ta bort dessa personuppgifter, särskilt på internet. Den registrerade bör kunna utöva denna rätt även när han eller hon inte längre är barn. Ytterligare lagring av personuppgifterna bör dock vara laglig, om detta krävs för att utöva yttrandefrihet och informationsfrihet, för att uppfylla en rättslig förpliktelse, för att utföra en uppgift i av allmänt intresse eller som ett led i myndighetsutövning som anförtrotts 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 inbegripa 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 uppmuntras att utveckla kompatibla format som möjliggör dataportabilitet. Denna rättighet bör vara tillämplig om den registrerade har tillhandahållit uppgifterna efter att ha lämnat sitt samtycke eller om behandlingen är nödvändig för att ett avtal ska kunna genomföras. Den bör inte vara tillämplig om behandlingen utgår från en annan rättslig grund än samtycke eller avtal. På grund av sin art bör denna rättighet inte utövas mot personuppgiftsansvariga som behandlar personuppgifter som ett led i myndighetsutövning. Därför bör den inte vara tillämplig när behandlingen av personuppgifterna är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning som utförs av den personuppgiftsansvarige. Den registrerades rätt att överföra eller motta personuppgifter som rör honom eller henne innebär inte någon skyldighet för de personuppgiftsansvariga att införa eller upprätthålla behandlingssystem som är tekniskt kompatibla. Om mer än en registrerad berörs inom en viss uppsättning personuppgifter, bör rätten att motta personuppgifterna inte inverka på andra registrerades rättigheter och friheter enligt denna förordning. Denna rättighet bör inte heller påverka den registrerades rätt att få till stånd radering av personuppgifter och de inskränkningar av denna rättighet vilka anges i denna förordning och bör i synnerhet inte medföra radering av personuppgifter om den registrerade som denne har lämnat för genomförande av ett avtal, i den utsträckning och så länge som personuppgifterna krävs för genomförande av avtalet. Om det är tekniskt möjligt, bör den registrerade ha rätt till direkt överföring av personuppgifterna från en personuppgiftsansvarig till en annan.

(69) När personuppgifter lagligen får behandlas, eftersom behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i en myndighetsutövning som utförs av den personuppgiftsansvarige, eller på grund av en personuppgiftsansvarigs eller en tredje parts berättigade intressen, bör alla registrerade ändå ha rätt att göra invändningar mot behandling av personuppgifter som rör de registrerades särskilda situation. Det bör ankomma på den personuppgiftsansvarige att visa att dennes tvingande berättigade intressen väger tyngre än den registrerades intressen eller grundläggande rättigheter och friheter.

(70) Om personuppgifter behandlas för direktmarknadsföring, bör den registrerade, oavsett om det handlar om inledande eller ytterligare behandling, ha rätt att när som helst kostnadsfritt invända mot sådan behandling, inbegripet profilering, i den mån denna är kopplad till direktmarknadsföring. Denna rättighet bör uttryckligen meddelas den registrerade och redovisas tydligt, klart och åtskilt från annan information.

(71) Den registrerade bör ha rätt att inte bli föremål för ett beslut, vilket kan inbegripa en åtgärd, med bedömning av personliga aspekter rörande honom eller henne, vilket enbart grundas på automatiserad behandling och medför rättsverkan för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne, såsom ett automatiserat avslag på en kreditansökan online eller e-rekrytering utan personlig kontakt. Sådan behandling omfattar ”profilering” i form av automatisk behandling av personuppgifter med bedömning av personliga aspekter rörande en fysisk person, särskilt för att analysera eller förutse aspekter avseende den registrerades arbetsprestation, ekonomiska situation, hälsa, personliga preferenser eller intressen, pålitlighet eller beteende, vistelseort eller förflyttningar, i den mån dessa har rättsverkan rörande honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne. Beslutsfattande grundat på sådan behandling, inbegripet profilering, bör dock tillåtas när det uttryckligen beviljas genom unionsrätten eller medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av, inbegripet för sådan övervakning och sådant förebyggande av bedrägerier och skatteundandragande som genomförs i enlighet med unionsinstitutionernas eller de nationella tillsynsorganens bestämmelser, standarder och rekommendationer samt för att sörja för tillförlitlighet hos en tjänst som tillhandahålls av den personuppgiftsansvarige, eller när det krävs för ingående eller genomförande av ett avtal mellan den registrerade och en personuppgiftsansvarig eller den registrerade har gett sitt uttryckliga samtycke. Denna form av uppgiftsbehandling bör under alla omständigheter omgärdas av lämpliga skyddsåtgärder, som bör inkludera specifik information till den registrerade och rätt till mänskligt ingripande, att framföra sina synpunkter, att erhålla en förklaring till det beslut som fattas efter sådan bedömning och att överklaga beslutet. Sådana åtgärder bör inte gälla barn.

I syfte att sörja för rättvis och transparent behandling med avseende på den registrerade, med beaktande av omständigheterna och det sammanhang i vilket personuppgifterna behandlas, bör den personuppgiftsansvarige använda adekvata matematiska eller statistiska förfaranden för profilering, genomföra tekniska och organisatoriska åtgärder som framför allt säkerställer att faktorer som kan medföra felaktigheter i personuppgifter korrigeras och att risken för fel minimeras samt säkra personuppgifterna på sådant sätt att man beaktar potentiella risker för den registrerades intressen och rättigheter och förhindrar bland annat diskriminerande effekter för fysiska personer, på grund av ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse, medlemskap i fackföreningar, genetisk status eller hälsostatus eller sexuell läggning, eller som leder till åtgärder som får sådana effekter. Automatiserat beslutsfattande och profilering baserat på särskilda kategorier av personuppgifter bör endast tillåtas på särskilda villkor.

(72) Profilering omfattas av denna förordnings bestämmelser om behandling av personuppgifter, såsom de rättsliga grunderna för behandlingen och principer för dataskydd. Europeiska dataskyddsstyrelsen som inrättas genom denna förordning (nedan kallad *styrelsen*) bör kunna utfärda riktlinjer i detta avseende.

(73) Begränsningar med avseende på specifika principer och rätten till information, tillgång till och rättelse eller radering av personuppgifter, rätten till dataportabilitet, rätten att göra invändningar, profileringsbaserade beslut samt information till den registrerade om personuppgiftsincidenter och vissa av den personuppgiftsansvariges relaterade skyldigheter kan införas genom unionsrätten eller medlemsstaternas nationella rätt, i den mån de är nödvändiga och proportionella i ett demokratiskt samhälle för att upprätthålla den allmänna säkerheten, exempelvis för att skydda människoliv, särskilt vid naturkatastrofer eller katastrofer framkallade av människan, vid förebyggande, förhindrande, utredning och lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten eller överträdelser av etiska principer för reglerade yrken, vad gäller unionens eller en medlemsstats övriga viktiga mål av allmänt intresse, särskilt om de är av stort ekonomiskt eller finansiellt intresse för unionen eller en medlemsstat, förande av offentliga register som förs av hänsyn till ett allmänt intresse, ytterligare behandling av arkiverade personuppgifter för att tillhandahålla specifik information om politiskt beteende under tidigare totalitära regimer eller skydd av den registrerade eller andras rättigheter och friheter, inklusive socialt skydd, folkhälsa och humanitära skäl. Dessa begränsningar bör överensstämma med kraven i stadgan och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

(74) Personuppgiftsansvariga bör åläggas ansvaret för all behandling av personuppgifter som de utför eller som utförs på deras vägnar. Personuppgiftsansvariga bör särskilt vara skyldiga att vidta lämpliga och effektiva åtgärder och kunna visa att behandlingen är förenlig med denna förordning, även vad gäller åtgärdernas effektivitet. Man bör inom dessa åtgärder beakta behandlingens art, omfattning, sammanhang och ändamål samt risken för fysiska personers rättigheter och friheter.

(75) Risken för fysiska personers rättigheter och friheter, av varierande sannolikhetsgrad och allvar, kan uppkomma till följd av personuppgiftsbehandling som skulle kunna medföra fysiska, materiella eller immateriella skador, i synnerhet om behandlingen kan leda till diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, obehörigt hävande av pseudonymisering eller annan betydande ekonomisk eller social nackdel, om registrerade kan berövas sina rättigheter och friheter eller hindras att utöva kontroll över sina personuppgifter, om personuppgifter behandlas som avslöjar ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse eller medlemskap i fackförening, om genetiska uppgifter, uppgifter om hälsa eller sexualliv eller fällande domar i brottmål samt överträdelser eller därmed sammanhängande säkerhetsåtgärder behandlas, om personliga aspekter bedöms, framför allt analyser eller förutsägelser beträffande sådant som rör arbetsprestationer, ekonomisk ställning, hälsa, personliga preferenser eller intressen, tillförlitlighet eller beteende, vistelseort eller förflyttningar, i syfte att skapa eller använda personliga profiler, om det sker behandling av personuppgifter rörande sårbara fysiska personer, framför allt barn, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.

(76) Hur sannolik och allvarlig risken för den registrerades rättigheter och friheter är bör fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål. Risken bör utvärderas på grundval av en objektiv bedömning, genom vilken det fastställs huruvida uppgiftsbehandlingen inbegriper en risk eller en hög risk.

(77) Vägledning för den personuppgiftsansvariges eller personuppgiftsbiträdets 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 uppmanas att beakta rätten till dataskydd när sådana produkter, tjänster och applikationer utvecklas och utformas och att, med tillbörlig hänsyn till den tekniska utvecklingen, säkerställa att personuppgiftsansvariga och personuppgiftsbiträden 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 personuppgiftsbiträdenas 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 personuppgiftsbiträden 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 personuppgiftsbiträdena 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 överträdelser 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 personuppgiftsbiträdets vägnar och kan kontaktas av samtliga tillsynsmyndigheter. Företrädaren bör uttryckligen utses genom en skriftlig fullmakt från den personuppgiftsansvarige eller från personuppgiftsbiträdet att agera på dennes vägnar med avseende på dennes skyldigheter enligt denna förordning. Utnämningen av företrädaren inverkar inte på den personuppgiftsansvariges eller på personuppgiftsbiträdets ansvar enligt denna förordning. Företrädaren bör utföra sina uppgifter i enlighet med erhållen fullmakt från den personuppgiftsansvarige eller från personuppgiftsbiträdet, vilket inbegriper samarbete med de behöriga tillsynsmyndigheterna i fråga om alla åtgärder som vidtas för att sörja för efterlevnad av denna förordning. Den utsedda företrädaren bör underkastas verkställighetsförfaranden i händelse den personuppgiftsansvarige eller personuppgiftsbiträdet inte uppfyller sina skyldigheter.

(81) För att se till att kraven i denna förordning uppfylls vad gäller behandling som av ett personuppgiftsbiträde ska utföras på en personuppgiftsansvarigs vägnar ska den personuppgiftsansvarige, när denne anförtror behandling åt ett personuppgiftsbiträde, endast använda 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. Personuppgiftsbiträdets 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 personuppgiftsbiträdet och den personuppgiftsansvarige, där föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade anges, med beaktande av personuppgiftsbiträdets 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 personuppgiftsbiträdet 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 personuppgiftsbiträdet återlämna eller radera personuppgifterna, beroende på vad den personuppgiftsansvarige väljer, såvida inte lagring av personuppgifterna krävs enligt den unionsrätt eller medlemsstaternas nationella rätt som personuppgiftsbiträdet 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 dennas begäran göra detta register tillgängligt, så att det kan tjäna som grund för övervakningen av behandlingen.

(83) För att upprätthålla säkerheten och förhindra behandling som bryter mot denna förordning bör personuppgiftsansvariga eller 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 överförts, lagrats eller på annat sätt behandlats, framför allt när denna kan medföra fysisk, materiell eller immateriell skada.

(84) I syfte att sörja för bättre efterlevnad av denna förordning när behandlingen sannolikt kan innebära en hög risk för fysiska personers rättigheter och friheter, bör den personuppgiftsansvarige vara ansvarig för att en konsekvensbedömning utförs avseende datasskydd för att bedöma framför allt riskens ursprung, art, särdrag och allvar. Resultatet av denna bedömning bör beaktas vid fastställandet av de lämpliga åtgärder som ska vidtas för att visa att behandlingen av personuppgifter är förenlig med denna förordning. I de fall en konsekvensbedömning avseende dataskydd ger vid handen att uppgiftsbehandlingen medför en hög risk, som den personuppgiftsansvarige inte kan begränsa genom lämpliga åtgärder med avseende på tillgänglig teknik och genomförandekostnader, bör ett samråd med tillsynsmyndigheten ske före behandlingen.

(85) En personuppgiftsincident som inte snabbt åtgärdas på lämpligt sätt kan för fysiska personer leda till fysisk, materiell eller immateriell skada, såsom förlust av kontrollen över de egna personuppgifterna eller till begränsning av deras rättigheter, diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, obehörigt hävande av pseudonymisering, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, eller till annan ekonomisk eller social nackdel för den berörda fysiska personen. Så

snart en personuppgiftsansvarig blir medveten om att en personuppgiftsincident har inträffat, bör den personuppgiftsansvarige därför anmäla personuppgiftsincidenten till tillsynsmyndigheten utan onödigt dröjsmål och, om så är möjligt, inom 72 timmar efter att ha blivit medveten om denna, om inte den personuppgiftsansvarige, i enlighet med ansvarsprincipen, kan påvisa att det är osannolikt att personuppgiftsincidenten kommer att medföra en risk för fysiska personers rättigheter och friheter. Om en sådan anmälan inte kan ske inom 72 timmar, bör skälen till fördröjningen åtfölja anmälan och information får lämnas i omgångar utan otillbörligt vidare dröjsmål.

(86) Den personuppgiftsansvarige bör utan onödigt dröjsmål underrätta den registrerade om en personuppgiftsincident, om personuppgiftsincidenten sannolikt kommer att medföra en hög risk för den fysiska personens rättigheter och friheter, så att denne kan vidta nödvändiga försiktighetsåtgärder. Denna underrättelse bör beskriva personuppgiftsincidentens art samt innehålla rekommendationer för den berörda fysiska personen om hur de potentiella negativa effekterna kan mildras. De registrerade bör underrättas så snart detta rimligtvis är möjligt, i nära samarbete med tillsynsmyndigheten och i enlighet med den vägledning som lämnats av den eller andra relevanta myndigheter, exempelvis brottsbekämpande myndigheter. Till exempel kräver behovet av att mildra en omedelbar skaderisk att de registrerade underrättas omedelbart, medan behovet av att vidta lämpliga åtgärder vid 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 anmälningsskyldigheter bör därför avskaffas och ersättas av effektiva förfaranden och mekanismer som i stället inriktas på de typer av behandlingar som sannolikt innebär en hög risk för fysiska personers rättigheter och friheter, i kraft av deras art, omfattning, sammanhang och ändamål. Dessa behandlingar kan vara sådana som särskilt inbegriper användning av ny teknik eller är av en ny typ, för vilken konsekvensbedömning avseende uppgiftsskydd inte tidigare har genomförts av den personuppgiftsansvarige, eller som blir nödvändiga på grund av den tid som har förflutit sedan den ursprungliga behandlingen.

(90) I sådana fall bör den personuppgiftsansvarige före behandlingen, med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt upphovet till risken, göra en konsekvensbedömning avseende dataskydd i syfte att bedöma den höga riskens specifika sannolikhetsgrad och allvar samt dess ursprung. Konsekvensbedömningen bör främst innefatta de planerade åtgärder, skyddsåtgärder och mekanismer som ska minska denna risk, säkerställa personuppgiftskyddet och visa att denna förordning efterlevs.

(91) Detta bör särskilt vara tillämpligt på storskalig uppgiftsbehandling med syftet att behandla betydande mängder personuppgifter på regional, nationell eller övernationell nivå, vilket skulle kunna påverka ett stort antal registrerade och sannolikt kommer att innebära en hög risk, exempelvis till följd av uppgifternas känsliga natur, där i enlighet med den uppnådda nivån av teknisk kunskap en ny teknik används storskaligt, samt på annan behandling som innebär en hög risk för registrerades rättigheter och friheter, framför allt när denna behandling gör det svårare för de registrerade att utöva sina rättigheter. En konsekvensbedömning avseende dataskydd bör

också göras, där personuppgifter behandlas i syfte att fatta beslut om specifika fysiska personer efter en systematisk och omfattande bedömning av fysiska personers personliga aspekter på grundval av profilering av dessa uppgifter eller efter behandling av särskilda kategorier av personuppgifter, biometriska uppgifter eller uppgifter om fällande domar i brottmål samt överträdelser eller därmed sammanhängande säkerhetsåtgärder. Likaså krävs en konsekvensbedömning avseende dataskydd för övervakning av allmän plats i stor omfattning, särskilt vid användning av optisk-elektroniska anordningar, eller för all annan behandling där den behöriga tillsynsmyndigheten anser att behandlingen sannolikt kommer att innebära en hög risk för de registrerades rättigheter och friheter, framför allt på grund av att den hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal eller på grund av att den systematiskt genomförs i stor omfattning. Behandling av personuppgifter bör inte anses vara storskalig, om det är fråga om personuppgifter från patienter eller klienter som behandlas av enskilda läkare, andra yrkesverksamma på hälsoområdet eller juridiska ombud. I dessa fall bör en konsekvensbedömning avseende dataskydd inte vara obligatorisk.

(92) Ibland kan det vara förnuftigt och ekonomiskt att en konsekvensbedömning avseende dataskydd inriktar sig på ett vidare område än ett enda projekt, exempelvis när myndigheter eller organ avser att skapa en gemensam tillämpnings- eller behandlingsplattform eller när flera personuppgiftsansvariga planerar att införa en gemensam tillämpnings- eller behandlingsmiljö för en hel bransch eller ett helt segment eller för en allmänt utnyttjad horisontell verksamhet.

(93) Medlemsstaterna kan anse det nödvändigt att genomföra en sådan bedömning före behandlingen i samband med antagandet av medlemsstaters nationella rätt som ligger till grund för utförandet av myndighetens eller det offentliga organets uppgifter och reglerar den aktuella specifika behandlingsåtgärden eller serien av åtgärder.

(94) Om det av en konsekvensbedömning avseende dataskydd framgår att behandlingen utan skyddsåtgärder, säkerhetsåtgärder och mekanismer för att minska risken kommer att innebära en hög risk för fysiska personers rättigheter och friheter, och den personuppgiftsansvarige anser att risken inte kan begränsas genom åtgärder som är rimliga med avseende på tillgänglig teknik och genomförandekostnader, bör samråd hållas med tillsynsmyndigheten innan behandlingen inleds. En sådan hög risk kommer sannolikt att orsakas av vissa typer av behandling samt av en viss omfattning och frekvens för behandlingen, vilket även kan leda till skador för eller kränkningar av fysiska personers rättigheter och friheter. Tillsynsmyndigheten bör inom en fastställd tid svara på en begäran om samråd. Ett uteblivet svar från tillsynsmyndigheten inom denna tid bör dock inte hindra ett eventuellt ingripande från tillsynsmyndighetens sida i enlighet med dess uppgifter och befogenheter enligt denna förordning, inbegripet befogenheten att förbjuda behandling. Som en del av denna samrådsprocess får resultatet av en konsekvensbedömning avseende dataskydd som utförs med avseende på behandlingen i fråga överlämnas till tillsynsmyndigheten, framför allt de åtgärder som planeras för att minska risken för fysiska personers rättigheter och friheter.

(95) Personuppgiftsbiträdet bör vid behov och på begäran bistå den personuppgiftsansvarige med fullgörande av de skyldigheter som härrör från utförandet av konsekvensbedömningar avseende dataskydd och förhandssamråd med tillsynsmyndigheten.

(96) Ett samråd med tillsynsmyndigheten bör även ske som ett led i det förberedande arbetet med en lagstiftningsåtgärd som stadgar om behandling av personuppgifter i syfte att säkerställa att den avsedda behandlingen överensstämmer med denna förordning och framför allt för att minska den risk den medför för den registrerade.

(97) När en behandling utförs av en myndighet, med undantag av domstolar eller oberoende rättsliga myndigheter som en del av deras dömande verksamhet, eller när en behandling utförs i den privata sektorn av en personuppgiftsansvarig vars kärnverksamhet består av behandlingsverksamhet som kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning, eller när den personuppgiftsansvariges eller personuppgiftsbiträdets 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 skälig nivå av skydd för de registrerades grundläggande rättigheter.

(103) Kommissionen kan med verkan för hela unionen fastställa att ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland eller en internationell organisation erbjuder en adekvat dataskyddsnivå och på så sätt skapa rättslig säkerhet och enhetlighet i hela unionen vad gäller tredjelandet eller den internationella organisationen som anses tillhandahålla en sådan skyddsnivå. I dessa fall får överföringar av personuppgifter till det tredjelandet eller den internationella organisationen ske utan ytterligare tillstånd. Kommissionen kan också, efter att ha underrättat tredjelandet eller den internationella organisationen och lämnat en fullständig motivering, besluta att ett sådant beslut ska återkallas.

(104) I enlighet med de grundläggande värderingar som unionen bygger på, bl.a. skyddet av mänskliga rättigheter, bör kommissionen i sin bedömning av tredjelandet eller ett territorium eller en specificerad sektor i ett tredjeland beakta hur ett visst tredjeland respekterar rättsstatsprincipen, tillgången till rättslig prövning samt internationella människorättsnormer och -standarder samt landets allmänna lagstiftning och sektorslagstiftning, inklusive lagstiftning om allmän säkerhet, försvar och nationell säkerhet samt allmän ordning och straffrätt. Vid antagandet av ett beslut om adekvat skyddsnivå avseende ett territorium eller en specificerad sektor i ett tredjeland bör hänsyn tas till tydliga och objektiva kriterier, t.ex. specifik behandling och tillämpningsområdet för tillämpliga rättsliga standarder och gällande lagstiftning i tredjelandet. Tredjelandet bör erbjuda garantier som säkerställer en

tillfredsställande skyddsnivå som i huvudsak motsvarar den som säkerställs i unionen, i synnerhet när personuppgifter behandlas inom en eller flera specifika sektorer. Tredjelandet bör framför allt säkerställa en effektiv oberoende dataskyddsövervakning och sörja för samarbetsmekanismer med medlemsstaternas dataskyddsmyndigheter, och de registrerade bör tillförsäkras effektiva och lagstadgade rättigheter samt effektiv administrativ och rättslig prövning.

(105) Utöver de internationella åtaganden som tredjelandet eller den internationella organisationen har gjort bör kommissionen beakta de skyldigheter som följer av tredjelandets eller den internationella organisationens deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter och genomförandet av dessa skyldigheter. Framför allt bör tredjelandets anslutning till Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk behandling av personuppgifter och dess tilläggsprotokoll beaktas. Kommissionen bör samråda med styrelsen vid bedömningen av skyddsnivån i tredjeländer eller internationella organisationer.

(106) Kommissionen bör övervaka hur beslut om skyddsnivå i ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland eller en internationell organisation fungerar, och övervaka hur beslut som antas på grundval av artikel 25.6 eller 26.4 i direktiv 95/46/EG fungerar. Kommissionen bör i sina beslut om adekvat skyddsnivå föreskriva en mekanism för periodisk översyn av hur de fungerar. Denna periodiska översyn bör genomföras i samråd med det berörda tredjelandet eller den berörda internationella organisationen, med beaktande av all relevant utveckling i tredjelandet eller den internationella organisationen. Vid övervakningen och genomförandet av den periodiska översynen bör kommissionen ta hänsyn till synpunkter och resultat från Europaparlamentet och rådet samt andra relevanta organ och källor. Kommissionen bör inom rimlig tid utvärdera hur de sistnämnda besluten fungerar och rapportera alla relevanta resultat till den kommitté, i den mening som avses i Europaparlamentets och rådets förordning (EU) nr 182/2011 [1], som inrättats enligt denna förordning och till Europaparlamentet och rådet.

(107) Kommissionen kan konstatera att ett tredjeland, ett territorium eller en viss specificerad sektor i ett tredjeland eller en internationell organisation inte längre säkerställer en adekvat dataskyddsnivå. Överföring av personuppgifter till detta tredjeland eller till denna internationella organisation bör då förbjudas, såvida inte kraven i denna förordning avseende överföring med stöd av lämpliga skyddsåtgärder, inbegripet bindande företagsbestämmelser och undantag för särskilda situationer, är uppfyllda. I så fall bör det finnas möjlighet till samråd mellan kommissionen och dessa tredjeländer eller internationella organisationer. Kommissionen bör i god tid informera tredjelandet eller den internationella organisationen om skälen och inleda samråd med tredjelandet eller organisationen för att avhjälpa situationen.

(108) Saknas beslut om adekvat skyddsnivå bör den personuppgiftsansvarige eller personuppgiftsbiträdet vidta åtgärder för att kompensera för det bristande dataskyddet i ett tredjeland med hjälp av lämpliga skyddsåtgärder för den registrerade. Sådana lämpliga skyddsåtgärder kan bestå i tillämpning av bindande företagsbestämmelser, standardbestämmelser om dataskydd som antagits av kommissionen, standardbestämmelser om dataskydd som antagits av en tillsynsmyndighet eller avtalsbestämmelser som godkänts av en tillsynsmyndighet. Dessa skyddsåtgärder bör säkerställa iakttagande av de krav i fråga om dataskydd och registrerades rättigheter som är lämpliga för behandling inom unionen, inbegripet huruvida bindande rättigheter för de registrerade och effektiva rättsmedel är tillgängliga, inbegripet en faktisk rätt att föra talan på administrativ väg eller inför domstol och att kräva kompensation i unionen eller i ett tredjeland. De bör särskilt gälla överensstämmelse med allmänna principer för behandling av personuppgifter samt principerna om inbyggt dataskydd och dataskydd som standard. Överföring av uppgifter kan också utföras av offentliga myndigheter eller organ till offentliga myndigheter eller organ i tredjeländer eller internationella organisationer med motsvarande skyldigheter eller uppgifter, inbegripet på grundval av bestämmelser som ska införas i administrativa överenskommelser, t.ex. samförståndsavtal, som föreskriver verkställbara och faktiska rättigheter för de registrerade. Tillstånd från den behöriga tillsynsmyndigheten bör erhållas när skyddsåtgärder föreskrivs i icke rättsligt bindande administrativa arrangemang.

(109) Personuppgiftsansvarigas eller personuppgiftsbiträdens möjlighet att använda standardiserade dataskyddsbestämmelser som antagits av kommissionen eller av en tillsynsmyndighet bör inte hindra att de infogar

[1] Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

standardiserade dataskyddsbestämmelser i ett vidare avtal, såsom ett avtal mellan personuppgiftsbiträdet och ett annat personuppgiftsbiträde, eller lägger till andra bestämmelser eller ytterligare skyddsåtgärder, under förutsättning att de inte direkt eller indirekt står i strid med standardavtalsklausuler som antagits av kommissionen eller av en tillsynsmyndighet eller påverkar de registrerades grundläggande rättigheter eller friheter. Personuppgiftsansvariga och personuppgiftsbiträden bör uppmuntras att tillhandahålla ytterligare skyddsåtgärder via avtalsmässiga åtaganden som kompletterar de standardiserade skyddsbestämmelserna.

(110) En koncern eller en grupp av företag som deltar i en gemensam ekonomisk verksamhet bör kunna använda sig av godkända bindande företagsbestämmelser för sina internationella överföringar från unionen till organisationer inom samma koncern eller grupp av företag som deltar i en gemensam ekonomisk verksamhet, under förutsättning att företagsbestämmelserna inbegriper alla nödvändiga principer och bindande rättigheter som säkerställer lämpliga skyddsåtgärder för överföringar eller kategorier av överföringar av personuppgifter.

(111) Det bör införas bestämmelser som ger möjlighet att under vissa omständigheter göra överföringar, om den registrerade har lämnat sitt uttryckliga samtycke, när överföringen är tillfällig och nödvändig med hänsyn till ett avtal eller ett rättsligt anspråk, oavsett om detta sker inom ett rättsligt förfarande eller i ett administrativt eller utomrättsligt förfarande, inbegripet förfaranden inför tillsynsorgan. Det bör också införas bestämmelser som ger möjlighet till överföringar om viktiga allmänintressen fastställda genom unionsrätten eller medlemsstaternas nationella rätt så kräver eller när överföringen görs från ett register som inrättats genom lag och är avsett att konsulteras av allmänheten eller av personer med ett berättigat intresse. I sistnämnda fall bör en sådan överföring inte omfatta alla personuppgifter eller hela kategorier av uppgifter i registret, och överföringen bör endast göras när registret är avsett att vara tillgängligt för personer med ett berättigat intresse, på begäran av dessa personer eller om de själva är mottagarna, med full hänsyn till de registrerades intressen och grundläggande rättigheter.

(112) Dessa undantag bör främst vara tillämpliga på uppgiftsöverföringar som krävs och är nödvändiga med hänsyn till viktiga allmänintressen, exempelvis vid internationella utbyten av uppgifter mellan konkurrensmyndigheter, skatte- eller tullmyndigheter, 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 registrerades eller en annan persons vitala intressen, inklusive dennes fysiska integritet och liv, om den registrerade är oförmögen att ge sitt samtycke. Saknas beslut om adekvat skyddsnivå får unionsrätten eller medlemsstaternas nationella rätt med hänsyn till viktiga allmänintressen uttryckligen fastställa gränser för överföringen av särskilda kategorier av uppgifter till ett tredjeland eller en internationell organisation. Medlemsstaterna bör underrätta kommissionen om sådana bestämmelser. Varje överföring till en internationell humanitär organisation av personuppgifter rörande en registrerad som är fysiskt eller rättsligt förhindrad att ge sitt samtycke, i syfte att utföra en uppgift inom ramen för Genèvekonventionerna eller vara förenlig med internationell humanitär rätt, vilken är tillämplig vid väpnade konflikter, skulle kunna anses vara nödvändig för ett betydande allmänintresse eller för att den är av vitalt intresse för den registrerade.

(113) Överföringar som kan anses vara icke återkommande och endast gäller ett begränsat antal registrerade kan också vara möjliga när personuppgiftsansvarigas tvingande berättigade intressen motiverar detta, om inte den registrerades intressen eller rättigheter och friheter väger tyngre än dessa intressen, och den personuppgiftsansvarige har bedömt alla omständigheter kring uppgiftsöverföringen. Den personuppgiftsansvarige bör ta särskild hänsyn till personuppgifternas art, den eller de avsedda behandlingarnas ändamål och varaktighet samt situationen i ursprungslandet, tredjelandet och det slutliga bestämmelselandet och bör tillhandahålla lämpliga åtgärder för att skydda fysiska personers grundläggande rättigheter och friheter vid behandlingen av deras personuppgifter. Sådana överföringar bör endast vara möjliga i vissa fall där inget av de andra skälen till överföring är tillämpligt. För vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör hänsyn tas till samhällets legitima förväntningar i fråga om ökad kunskap. Den personuppgiftsansvarige bör informera tillsynsmyndigheten och den registrerade om överföringen.

(114) Om kommissionen inte har fattat beslut om adekvat dataskyddsnivå i ett tredjeland, bör den personuppgiftsansvarige eller personuppgiftsbiträdet i alla fall använda sig av lösningar som ger de registrerade verkställbara och effektiva rättigheter vad gäller behandlingen av deras personuppgifter inom unionen när dessa uppgifter väl har överförts, så att de fortsatt kan utöva sina grundläggande rättigheter och att skyddsåtgärder fortsatt gäller i förhållande till dem.

(115) Vissa tredjeländer antar lagar och andra författningar som syftar till att direkt reglera behandling som genomförs av fysiska och juridiska personer under medlemsstaternas jurisdiktion. Detta kan inkludera rättsliga avgöranden eller beslut av administrativa myndigheter i tredjeländer med krav på att personuppgiftsansvariga eller personuppgiftsbiträden överför eller överlämnar personuppgifter, vilka inte grundar sig på något gällande internationellt avtal, såsom ett fördrag om ömsesidig rättshjälp, mellan det begärande tredjelandet och unionen eller en medlemsstat. Extraterritoriell tillämpning av dessa lagar och andra författningar kan strida mot internationell rätt och inverka menligt på det skydd av fysiska personer som säkerställs inom unionen genom denna förordning. Överföringar bör endast tillåtas om villkoren i denna förordning för en överföring till tredjeländer är uppfyllda. Detta kan vara fallet bl.a. när utlämnande är nödvändigt på grund av ett viktigt allmänintresse som erkänns i unionsrätten eller i medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av.

(116) När personuppgifter förs över gränser utanför unionen kan detta öka risken för att fysiska personer inte kan utöva sina dataskyddsrättigheter, i synnerhet för att skydda sig från otillåten användning eller otillåtet utlämnande av denna information. Samtidigt kan tillsynsmyndigheter finna att de inte är i stånd att handlägga klagomål eller göra utredningar som gäller verksamheter utanför gränserna för deras land. Deras strävan att arbeta tillsammans över gränserna kan också hindras av otillräckliga preventiva eller korrigerande befogenheter, oenhetliga rättsliga regelverk och praktiska hinder, som exempelvis bristande resurser. Närmare samarbete mellan dataskyddstillsynsmyndigheter bör därför främjas för att hjälpa dem att utbyta information och utföra utredningar med sina internationella motparter. I syfte att bygga upp internationella samarbetsmekanismer för att underlätta och tillhandahålla ömsesidig internationell hjälp med att kontrollera efterlevnaden av lagstiftningen till skydd för personuppgifter, bör kommissionen och tillsynsmyndigheterna utbyta information och samarbeta, inom verksamhet som rör utövandet av deras befogenheter, med behöriga myndigheter i tredjeländer, på grundval av ömsesidighet och i överensstämmelse med denna förordning.

(117) Ett väsentligt inslag i skyddet av fysiska personer vid behandlingen av personuppgifter är att medlemsstaterna inrättar tillsynsmyndigheter med behörighet att utföra sina uppgifter och utöva sina befogenheter under fullständigt oberoende. Medlemsstaterna bör kunna inrätta fler än en tillsynsmyndighet om det behövs för att ta hänsyn till den egna konstitutionella, organisatoriska och administrativa strukturen.

(118) Tillsynsmyndigheternas oberoende bör dock inte innebära att deras utgifter inte kan underkastas kontroll- eller övervakningsmekanismer eller bli föremål för domstolsprövning.

(119) Om en medlemsstat inrättar flera tillsynsmyndigheter, bör den genom lagstiftning säkerställa att dessa tillsynsmyndigheter effektivt deltar i mekanismen för enhetlighet. Medlemsstaten bör i synnerhet utnämna en tillsynsmyndighet som fungerar som samlande kontaktpunkt för dessa myndigheters effektiva deltagande i mekanismen för att säkra ett snabbt och smidigt samarbete med övriga tillsynsmyndigheter, styrelsen och kommissionen.

(120) Varje tillsynsmyndighet bör tilldelas de ekonomiska och personella resurser och lokalutrymmen samt den infrastruktur som är nödvändig för att den effektivt ska kunna utföra sina uppgifter, däribland de uppgifter som är knutna till ömsesidigt bistånd och samarbete med övriga tillsynsmyndigheter i hela unionen. Varje tillsynsmyndighet bör ha en separat offentlig årlig budget, som kan ingå i den övergripande statsbudgeten eller nationella budgeten.

(121) De allmänna villkoren för tillsynsmyndighetens ledamot eller ledamöter bör fastställas genom varje medlemsstats lagstiftning och där bör i synnerhet föreskrivas att ledamöterna ska utnämnas genom ett öppet förfarande antingen av medlemsstatens parlament, regering eller statschef, på grundval av ett förslag från regeringen, en ledamot av regeringen, parlamentet eller en av parlamentets kammare eller av ett oberoende organ som enligt medlemsstaternas nationella rätt har anförtrotts 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 inbegripa att hantera klagomål som lämnas in av en registrerad, genomföra undersökningar om tillämpningen av denna förordning samt främja allmänhetens medvetenhet om risker, bestämmelser, skyddsåtgärder och rättigheter när det gäller behandlingen av personuppgifter.

(123) Tillsynsmyndigheterna bör övervaka tillämpningen av bestämmelserna i denna förordning och bidra till att tillämpningen blir enhetlig över hela unionen, för att skydda fysiska personer vid behandling av deras personuppgifter och för att underlätta det fria flödet av personuppgifter inom den inre marknaden. För detta ändamål bör tillsynsmyndigheterna samarbeta såväl sinsemellan som med kommissionen, utan att det behövs något avtal mellan medlemsstaterna om tillhandahållande av ömsesidigt bistånd eller om sådant samarbete.

(124) Om behandlingen av personuppgifter sker inom ramen för verksamhet vid en personuppgiftsansvarigs eller ett 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 överträdelser av denna förordning och delta i rättsliga förfaranden. Dessa befogenheter bör även omfatta en befogenhet att införa en tillfällig eller definitiv begränsning av, inklusive förbud mot, behandling. Medlemsstaterna får fastställa andra uppgifter med anknytning till skyddet av personuppgifter enligt denna förordning. Tillsynsmyndigheternas befogenheter bör utövas opartiskt, rättvist och inom rimlig tid i överensstämmelse med lämpliga rättssäkerhetsgarantier i unionsrätten och i medlemsstaternas nationella rätt. Framför allt bör varje åtgärd vara lämplig, nödvändig och proportionell för att säkerställa efterlevnad av denna förordning, med beaktande av omständigheterna i varje enskilt fall, samt respektera varje persons rätt att bli hörd innan några enskilda åtgärder som påverkar honom eller henne negativt vidtas och vara utformad så att onödiga kostnader och alltför stora olägenheter för de berörda personerna undviks. Undersökningsbefogenheten när det gäller tillträde till lokaler bör utövas i enlighet med särskilda krav i medlemsstaternas nationella processrätt, såsom kravet på att inhämta förhandstillstånd från rättsliga myndigheter. Varje rättsligt bindande åtgärd som vidtas av tillsynsmyndigheten bör vara skriftlig, klar och entydig, innehålla information om vilken tillsynsmyndighet som har utfärdat åtgärden och datum för utfärdandet, vara undertecknad av tillsynsmyndighetens chef eller en av dess ledamöter efter dennes bemyndigande samt innehålla en motivering till åtgärden och en hänvisning till rätten till ett effektivt rättsmedel. Detta bör inte utesluta ytterligare krav enligt medlemsstaternas nationella processrätt. Antagande av ett rättsligt bindande beslut innebär att det kan bli föremål för domstolsprövning i den medlemsstat till vilken den tillsynsmyndighet som antog beslutet hör.

(130) Om den tillsynsmyndighet till vilken klagomålet har ingetts inte är den ansvariga tillsynsmyndigheten, bör den ansvariga tillsynsmyndigheten nära samarbeta med den tillsynsmyndighet till vilken klagomålet har ingetts i enlighet med de bestämmelser om samarbete och enhetlighet som fastställs i denna förordning. I sådana fall bör den ansvariga tillsynsmyndigheten när den vidtar åtgärder avsedda att ha rättsverkan, inbegripet utdömandet av administrativa sanktionsavgifter, ta största hänsyn till synpunkter från den tillsynsmyndighet till vilken klagomålet har ingetts, vilken bör kvarstå som behörig för genomförande av utredningar på den egna medlemsstatens territorium i samverkan med den behöriga tillsynsmyndigheten.

(131) Om en annan tillsynsmyndighet bör agera som ansvarig tillsynsmyndighet för den personuppgiftsansvariges eller 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 stadgeenliga mål av allmänt intresse och bedriver verksamhet på området skydd av personuppgifter, att på hans eller hennes vägnar lämna in ett klagomål till en tillsynsmyndighet, om detta föreskrivs i medlemsstatens nationella rätt, att på den registrerades vägnar utöva rätten till domstolsprövning eller att på den registrerades vägnar utöva rätten att ta emot ersättning. En medlemsstat får föreskriva att ett sådant organ, en sådan organisation eller en sådan sammanslutning ska ha rätt att lämna in ett klagomål i den medlemsstaten, oberoende av en registrerad persons mandat, och ha rätt till ett effektivt rättsmedel, om det eller den har skäl att anse att en registrerad persons rättigheter har kränkts till följd av behandling av personuppgifter som strider mot denna förordning. Detta organ, denna organisation eller denna sammanslutning får inte ges rätt att kräva ersättning på en registrerad persons vägnar oberoende av den registrerades mandat.

(143) Varje fysisk eller juridisk person har rätt att väcka ogiltighetstalan mot styrelsens beslut vid domstolen enligt de villkor som föreskrivs i artikel 263 i EUF-fördraget. I sin egenskap av adressater för sådana beslut måste, i enlighet med artikel 263 i EUF-fördraget, de berörda tillsynsmyndigheter som önskar överklaga dessa väcka talan inom två månader efter det att beslutet meddelats dem. Om styrelsens beslut direkt och personligen berör en personuppgiftsansvarig, ett personuppgiftsbiträde eller en enskild, kan den enskilde väcka ogiltighetstalan mot 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 meddelar ett förhandsavgörande om tolkningen av unionsrätten, inbegripet denna förordning. Om dessutom ett beslut av en tillsynsmyndighet om genomförande av ett beslut av styrelsen överklagas till en nationell domstol och giltigheten av styrelsens beslut ifrågasätts, har inte den nationella domstolen befogenhet att förklara styrelsens beslut ogiltigt utan måste hänskjuta frågan om giltighet till domstolen i enlighet med artikel 267 i EUF-fördraget såsom den tolkats av domstolen, närhelst den anser att beslutet är ogiltigt. En nationell domstol får dock inte hänskjuta en fråga om giltigheten av styrelsens beslut på begäran av en fysisk eller juridisk person som haft tillfälle att väcka ogiltighetstalan mot beslutet, i synnerhet inte om denna person direkt och personligen berördes av beslutet men inte gjorde detta inom den frist som anges i artikel 263 i EUF-fördraget.

(144) Om en domstol där ett förfarande inletts mot beslut som har fattats av en tillsynsmyndighet har skäl att tro att ett förfarande rörande samma behandling, såsom samma sakfråga vad gäller behandling av samma personuppgiftsansvarige eller samma personuppgiftsbiträde, eller samma händelseförlopp, har inletts vid en annan behörig domstol i en annan medlemsstat, bör den kontakta denna domstol i syfte att bekräfta förekomsten av sådana relaterade förfaranden. Om relaterade förfaranden pågår vid en domstol i en annan medlemsstat får alla andra

domstolar än den domstol där förfarandet först inleddes låta förfarandena vila eller på en av parternas begäran förklara sig obehöriga till förmån för den domstol där förfarandet först inleddes, om den domstolen har behörighet i förfarandet i fråga och dess lagstiftning tillåter förening av sådana relaterade förfaranden. Förfarandena anses vara relaterade, om de är så nära förenade att en gemensam handläggning och dom är påkallad för att undvika att oförenliga domar meddelas som en följd av att förfarandena prövas i olika rättegångar.

(145) När det gäller ett rättsligt förfarande mot en personuppgiftsansvarig eller ett personuppgiftsbiträde bör käranden kunna välja att väcka talan antingen vid domstolarna i de medlemsstater där den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad eller där den registrerade är bosatt, såvida inte den personuppgiftsansvarige är en myndighet i en medlemsstat som agerar inom ramen för sin myndighetsutövning.

(146) Den personuppgiftsansvarige eller personuppgiftsbiträdet bör ersätta all skada som en person kan komma att lida till följd av behandling som strider mot denna förordning. Den personuppgiftsansvarige eller personuppgiftsbiträdet bör dock befrias från skadeståndsskyldighet om den kan visa att den inte på något sätt är ansvarig för skadan. Begreppet skada bör tolkas brett mot bakgrund av domstolens rättspraxis på ett sätt som fullt ut återspeglar denna förordnings mål. Detta påverkar inte skadeståndsanspråk till följd av överträdelser av andra bestämmelser i unionsrätten eller i medlemsstaternas nationella rätt. Behandling som strider mot denna förordning omfattar även behandling som strider mot delegerade akter och 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 ([1]), påverka tillämpningen av sådana särskilda bestämmelser.

(148) För att stärka verkställigheten av denna förordning bör det utdömas sanktioner, inbegripet administrativa sanktionsavgifter, för överträdelser av denna förordning utöver eller i stället för de lämpliga åtgärder som tillsynsmyndigheten vidtar i enlighet med denna förordning. Vid en mindre överträdelse eller om den sanktionsavgift som sannolikt skulle utdömas skulle innebära en oproportionell börda för en fysisk person får en reprimand utfärdas i stället för sanktionsavgifter. Vederbörlig hänsyn bör dock tas till överträdelsens karaktär, svårighetsgrad och varaktighet och huruvida den har skett uppsåtligen, vilka åtgärder som vidtagits för att lindra skadan, graden av ansvar eller eventuella tidigare överträdelser av relevans, det sätt på vilket överträdelsen kom till tillsynsmyndighetens kännedom, efterlevnad av åtgärder som förordnats mot den personuppgiftsansvarige eller personuppgiftsbiträdet, tillämpning av en uppförandekod och eventuella andra försvårande eller förmildrande faktorer. Utdömandet av sanktioner, inbegripet administrativa sanktionsavgifter, bör underkastas adekvata rättssäkerhetsgarantier i överensstämmelse med allmänna principer inom unionsrätten och stadgan, vilket inbegriper ett effektivt rättsligt skydd och korrekt rättsligt förfarande.

(149) Medlemsstaterna bör kunna fastställa bestämmelser om straffrättsliga påföljder för överträdelser av denna förordning, inbegripet för överträdelser av nationella bestämmelser som antagits i enlighet med och inom ramen för denna förordning. Dessa straffrättsliga påföljder kan även inbegripa en möjlighet att förverka den vinning som gjorts genom överträdelser av denna förordning. Utdömandet av straffrättsliga påföljder för överträdelser av sådana nationella bestämmelser och administrativa sanktioner bör dock inte medföra ett åsidosättande av principen ne bis in idem enligt domstolens tolkning.

(150) För att förstärka och harmonisera de administrativa sanktionerna för överträdelser av denna förordning bör samtliga tillsynsmyndigheter ha befogenhet att utfärda administrativa sanktionsavgifter. Det bör i denna

([1]) Europaparlamentets och rådets förordning (EU) nr 1215/2012 av den 12 december 2012 om domstols behörighet och om erkännande och verkställighet av domar på privaträttens område (EUT L 351, 20.12.2012, s. 1).

förordning anges vilka överträdelserna är, den övre gränsen för och kriterierna för fastställande av de administrativa sanktionsavgifterna, som i varje enskilt fall bör bestämmas av den behöriga tillsynsmyndigheten med beaktande av alla relevanta omständigheter i det särskilda fallet, med vederbörlig hänsyn bl.a. till överträdelsens karaktär, svårighetsgrad och varaktighet samt till dess följder och till de åtgärder som vidtas för att sörja för fullgörandet av skyldigheterna enligt denna förordning och för att förebygga eller lindra konsekvenserna av överträdelsen. Om de administrativa sanktionsavgifterna åläggs ett företag, bör ett företag i detta syfte anses vara ett företag i den mening som avses i artiklarna 101 och 102 i EUF-fördraget. Om de administrativa sanktionsavgifterna åläggs personer som inte är ett företag, bör tillsynsmyndigheten ta hänsyn till den allmänna inkomstnivån i medlemsstaten och personens ekonomiska situation, när den överväger lämplig sanktionsavgift. Mekanismen för enhetlighet kan också tillämpas för att främja en enhetlig tillämpning av administrativa sanktionsavgifter. Medlemsstaterna bör fastställa om och i vilken utsträckning myndigheter ska omfattas av administrativa sanktionsavgifter. Utfärdande av administrativa sanktionsavgifter eller utdelning av en varning påverkar inte tillämpningen av tillsynsmyndigheternas övriga befogenheter eller av andra sanktioner enligt denna förordning.

(151) Danmarks och Estlands rättssystem tillåter inte administrativa sanktionsavgifter i enlighet med denna förordning. Bestämmelserna om administrativa sanktionsavgifter kan tillämpas så att sanktionsavgiften i Danmark utdöms som en straffrättslig påföljd av en behörig nationell domstol och att den i Estland utdöms av tillsynsmyndigheten inom ramen för ett förseelseförfarande, under förutsättning att en sådan tillämpning av bestämmelserna i dessa medlemsstater har en effekt som är likvärdig med administrativa sanktionsavgifter som utdöms av tillsynsmyndigheter. De behöriga nationella domstolarna bör därför beakta rekommendationen från den tillsynsmyndighet som initierar sanktionsavgiften. De sanktionsavgifter som utdöms bör i alla händelser vara effektiva, proportionella och avskräckande.

(152) Om denna förordning inte harmoniserar administrativa sanktioner eller om nödvändigt i andra fall, till exempel vid fall av allvarliga överträdelser av denna förordning, bör medlemsstaterna genomföra ett system med effektiva, proportionella och avskräckande sanktioner. Dessa sanktioners art, straffrättsliga eller administrativa, bör fastställas i medlemsstaternas nationella rätt.

(153) Medlemsstaterna bör i sin lagstiftning sammanjämka bestämmelserna om yttrandefrihet och informationsfrihet, vilket inbegriper journalistiska, akademiska, konstnärliga och/eller litterära uttrycksformer, med rätten till skydd av personuppgifter i enlighet med denna förordning. Behandling av personuppgifter enbart för journalistiska, akademiska, konstnärliga eller litterära ändamål bör undantas från vissa av kraven i denna förordning, så att rätten till skydd av personuppgifter vid behov kan förenas med rätten till yttrandefrihet och informationsfrihet, som följer av artikel 11 i stadgan. Detta bör särskilt gälla vid behandling av personuppgifter inom det audiovisuella området och i nyhetsarkiv och pressbibliotek. Medlemsstaterna bör därför anta lagstiftningsåtgärder som fastställer de olika undantag som behövs för att skapa en balans mellan dessa grundläggande rättigheter. Medlemsstaterna bör fastställa sådana undantag med avseende på allmänna principer, de registrerades rättigheter, personuppgiftsansvariga och personuppgiftsbiträden, överföring av uppgifter till tredjeländer eller internationella organisationer, de oberoende tillsynsmyndigheterna, samarbete och enhetlighet samt specifika situationer där personuppgifter behandlas. Om sådana undantag varierar från en medlemsstat till en annan, ska den nationella rätten i den medlemsstat vars lag den personuppgiftsansvarige omfattas av tillämpas. För att beakta vikten av rätten till yttrandefrihet i varje demokratiskt samhälle måste det göras en bred tolkning av vad som innefattas i denna frihet, som till exempel journalistik.

(154) Denna förordning gör det möjligt att vid tillämpningen av den ta hänsyn till principen om allmänhetens rätt att få tillgång till allmänna handlingar. Allmänhetens rätt att få tillgång till allmänna handlingar kan betraktas som ett allmänt intresse. Personuppgifter i handlingar som innehas av en myndighet eller ett offentligt organ bör kunna lämnas ut offentligt av denna myndighet eller detta organ, om utlämning stadgas i unionsrätten eller i medlemsstatens nationella rätt som är tillämplig på myndigheten eller det offentliga organet. Denna rätt bör sammanjämka allmänhetens rätt att få tillgång till allmänna handlingar och vidareutnyttjande av information från den offentliga sektorn med rätten till skydd av personuppgifter och får därför innehålla föreskrifter om den nödvändiga sammanjämkningen med rätten till skydd av personuppgifter enligt denna förordning. Hänvisningen till offentliga myndigheter och organ bör i detta sammanhang omfatta samtliga myndigheter eller andra organ som omfattas av medlemsstaternas nationella rätt om allmänhetens tillgång till handlingar. Europaparlamentets och rådets direktiv 2003/98/EG ([1]) ska inte på något sätt påverka skyddsnivån för fysiska personer med avseende

([1]) Europaparlamentets och rådets direktiv 2003/98/EG av den 17 november 2003 om vidareutnyttjande av information från den offentliga sektorn (EUT L 345, 31.12.2003, s. 90).

på behandling av personuppgifter enligt bestämmelserna i unionsrätten och i medlemsstaternas nationella rätt och i synnerhet ändras inte de skyldigheter och rättigheter som anges i denna förordning genom det direktivet. I synnerhet ska direktivet inte vara tillämpligt på handlingar till vilka, med hänsyn till skyddet av personuppgifter, tillgång enligt tillgångsbestämmelserna är utesluten eller begränsad eller på delar av handlingar som är tillgängliga enligt dessa bestämmelser men som innehåller personuppgifter vilkas vidareutnyttjande i lag har fastställts som oförenligt med lagstiftningen om skydd för fysiska personer vid behandling av personuppgifter.

(155) En medlemsstatsnationella rätt eller kollektivavtal, inbegripet ”verksamhetsöverenskommelser”, får föreskriva särskilda bestämmelser om behandling av anställdas personuppgifter i anställningsförhållanden, särskilt när det gäller villkoren för hur personuppgifter i anställningsförhållanden får behandlas på grundval av samtycke från den anställde, rekrytering, genomförande av anställningsavtalet, inklusive befrielse från i lag eller kollektivavtal stadgade skyldigheter, ledning, planering och organisering av arbetet samt hälsa och säkerhet på arbetsplatsen, men också när det gäller att såväl kollektivt som individuellt utöva och komma i åtnjutande av rättigheter och förmåner som är knutna till anställningen samt att avsluta anställningsförhållandet.

(156) Behandlingen av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör omfattas av lämpliga skyddsåtgärder för de registrerades rättigheter och friheter enligt denna förordning. Skyddsåtgärderna bör säkerställa att tekniska och organisatoriska åtgärder har införts för att se till att särskilt principen om uppgiftsminimering iakttas. Ytterligare behandling av personuppgifter för arkivändamål av allmänintresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör genomföras, när den personuppgiftsansvarige har bedömt möjligheten att uppnå dessa ändamål genom behandling av personuppgifter som inte medger eller inte längre medger identifiering av de registrerade, förutsatt att det finns lämpliga skyddsåtgärder (t. ex. pseudonymisering av personuppgifter). Medlemsstaterna bör införa lämpliga skyddsåtgärder för behandlingen av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Medlemsstaterna bör på särskilda villkor med förbehåll för lämpliga skyddsåtgärder för de registrerade ha rätt att specificera och göra undantag från kraven på information, rätten till rättelse eller radering av personuppgifter, rätten att bli bortglömd, rätten till begränsning av behandlingen, rätten till dataportabilitet och rätten att göra invändning i samband med behandling av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Villkoren och säkerhetsåtgärderna i fråga kan medföra att de registrerade måste följa särskilda förfaranden för att utöva dessa rättigheter, om det är lämpligt med hänsyn till den särskilda behandlingens syfte tillsammans med tekniska och organisatoriska åtgärder som syftar till att minimera behandlingen av personuppgifter i enlighet med principerna om proportionalitet och nödvändighet. Behandling av personuppgifter för vetenskapliga ändamål bör även vara förenlig med annan relevant lagstiftning, exempelvis om kliniska prövningar.

(157) Genom att koppla samman information från olika register kan forskare erhålla ny kunskap av stort värde med avseende på medicinska tillstånd som exempelvis hjärt-kärlsjukdomar, cancer och depression. På grundval av registren kan forskningsresultaten förbättras, eftersom de bygger på en större befolkningsgrupp. Forskning inom samhällsvetenskap som bedrivs på grundval av register gör det möjligt för forskare att få grundläggande kunskaper om sambandet på lång sikt mellan ett antal sociala villkor, exempelvis arbetslöshet och utbildning, och andra livsförhållanden. Forskningsresultat som erhållits på grundval av register utgör en stabil, högkvalitativ kunskap, som kan ligga till grund för utformningen och genomförandet av kunskapsbaserad politik, förbättra livskvaliteten för ett antal personer och förbättra de sociala tjänsternas effektivitet. För att underlätta vetenskaplig forskning får personuppgifter behandlas för vetenskapliga forskningsändamål, med förbehåll för lämpliga villkor och skyddsåtgärder i unionsrätten eller i medlemsstaternas nationella rätt.

(158) Om personuppgifter behandlas för arkivändamål, bör denna förordning också gälla denna behandling, med beaktande av att denna förordning inte bör gälla för avlidna personer. Offentliga myndigheter eller offentliga eller privata organ som innehar uppgifter av allmänt intresse bör vara tillhandahållare som, i enlighet med unionsrätten eller medlemsstaternas nationella rätt, har en rättslig skyldighet att förvärva, bevara, bedöma, organisera, beskriva, kommunicera, främja, sprida och ge tillgång till uppgifter av bestående värde för allmänintresset. Medlemsstaterna bör också ha rätt att föreskriva att personuppgifter får vidarebehandlas för arkivering, exempelvis i syfte att tillhandahålla specifik information om politiskt beteende under tidigare totalitära regimer, folkmord, brott mot mänskligheten, särskilt Förintelsen, eller krigsförbrytelser.

(159) Om personuppgifter behandlas för vetenskapliga forskningsändamål, bör denna förordning också gälla denna behandling. Behandling av personuppgifter för vetenskapliga forskningsändamål bör i denna förordning ges en vid tolkning och omfatta till exempel teknisk utveckling och demonstration, grundforskning, tillämpad forskning och privatfinansierad forskning. Behandlingen av personuppgifter bör dessutom ta hänsyn till unionens mål enligt artikel 179.1 i EUF-fördraget angående åstadkommandet av ett europeiskt forskningsområde. Vetenskapliga forskningsändamål bör också omfatta studier som utförs av ett allmänt intresse inom folkhälsoområdet. För att tillgodose de särskilda kraven i samband med behandling av personuppgifter för vetenskapliga forskningsändamål bör särskilda villkor gälla, särskilt vad avser offentliggörande eller annat utlämnande av personuppgifter inom ramen för vetenskapliga forskningsändamål. Om resultatet av vetenskaplig forskning, särskilt för hälso- och sjukvårdsändamål, ger anledning till ytterligare åtgärder i den registrerades intresse, bör de allmänna reglerna i denna förordning tillämpas på dessa åtgärder.

(160) Om personuppgifter behandlas för historiska forskningsändamål, bör denna förordning också gälla denna behandling. Detta bör även omfatta forskning för historiska och genealogiska ändamål, med beaktande av att denna förordning inte bör gälla för avlidna personer.

(161) När det gäller samtycke till deltagande i vetenskaplig forskning inom ramen för kliniska prövningar, bör de relevanta bestämmelserna i Europaparlamentets och rådets förordning (EU) nr 536/2014 ([1]) tillämpas.

(162) Om personuppgifter behandlas för statistiska ändamål, bör denna förordning gälla denna behandling. Unionsrätten eller medlemsstaternas nationella rätt bör, inom ramen för denna förordning, fastställa statistiskt innehåll, kontroll av tillgång, specifikationer för behandling av personuppgifter för statistiska ändamål och lämpliga åtgärder till skydd för den registrerades rättigheter och friheter och för att säkerställa insynsskydd för statistiska uppgifter. Med statistiska ändamål avses varje åtgärd som vidtas för den insamling och behandling av personuppgifter som är nödvändig för statistiska undersökningar eller för framställning av statistiska resultat. Dessa statistiska resultat kan vidare användas för olika ändamål, inbegripet vetenskapliga forskningsändamål. Ett statistiskt ändamål innebär att resultatet av behandlingen för statistiska ändamål inte består av personuppgifter, utan av aggregerade personuppgifter, och att resultatet eller uppgifterna inte används till stöd för åtgärder eller beslut som avser en särskild fysiskperson.

(163) De konfidentiella uppgifter som unionens myndigheter och nationella statistikansvariga myndigheter samlar in för att framställa officiell europeisk och officiell nationell statistik bör skyddas. Europeisk statistik bör utvecklas, framställas och spridas i enlighet med de statistiska principerna i artikel 338.2 i EUF-fördraget, medan hanteringen av nationell statistik även bör överensstämma med medlemsstaternas nationella rätt. Europaparlamentets och rådets förordning (EG) nr 223/2009 ([2]) innehåller ytterligare preciseringar om statistisk konfidentialitet för europeisk statistik.

(164) Vad beträffar tillsynsmyndigheternas befogenheter att från personuppgiftsansvariga eller personuppgiftsbiträden få tillgång till personuppgifter och tillträde till lokaler, får medlemsstaterna, inom gränserna för denna förordning, genom lagstiftning anta särskilda regler för att skydda yrkesmässig eller annan motsvarande tystnadsplikt, i den mån detta är nödvändigt för att jämka samman rätten till skydd av personuppgifter med tystnadsplikten. Detta påverkar inte tillämpningen av medlemsstaternas befintliga skyldigheter att anta bestämmelser om tystnadsplikt, där detta krävs enligt unionsrätten.

(165) Denna förordning är förenlig med kravet på att respektera och inte påverka den ställning som kyrkor och religiösa sammanslutningar eller samfund har i medlemsstaterna enligt gällande grundlag i enlighet med artikel 17 i EUF-fördraget.

(166) I syfte att uppnå målen för denna förordning, nämligen att skydda fysiska personers grundläggande rättigheter och friheter och i synnerhet deras rätt till skydd av personuppgifter och för att säkra det fria flödet av

([1]) Europaparlamentets och rådets förordning (EU) nr 536/2014 av den 16 april 2014 om kliniska prövningar av humanläkemedel och om upphävande av direktiv 2001/20/EG (EUT L 158, 27.5.2014, s. 1).

([2]) Europaparlamentets och rådets förordning (EG) nr 223/2009 av den 11 mars 2009 om europeisk statistik och om upphävande av Europaparlamentets och rådets förordning (EG, Euratom) nr 1101/2008 om utlämnande av insynsskyddade statistiska uppgifter till Europeiska gemenskapernas statistikkontor, rådets förordning (EG) nr 322/97 om gemenskapsstatistik och rådets beslut 89/382/EEG, Euratom om inrättande av en kommitté för Europeiska gemenskapernas statistiska program (EUT L 87, 31.3.2009, s. 164).

personuppgifter inom unionen, bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen. Delegerade akter bör framför allt antas när det gäller kriterier och krav vad gäller certifieringsmekanismer, information som ska ges med användning av standardiserade symboler och förfaranden för att tillhandahålla sådana symboler. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå. När kommissionen förbereder och utarbetar delegerade akter bör den se till att relevanta handlingar översänds samtidigt till Europaparlamentet och rådet och att detta sker så snabbt som möjligt och på lämpligt sätt.

(167) För att säkerställa enhetliga villkor för tillämpningen av denna förordning bör kommissionen ges genomförandebefogenheter 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 skyndsamhet anta omedelbart tillämpliga genomförandeakter, när tillgängliga bevis visar att ett tredjeland, ett territorium eller en specificerad sektor inom det tredjelandet eller en internationell organisation inte upprätthåller en adekvat skyddsnivå.

(170) Eftersom målet för denna förordning, nämligen att säkerställa en likvärdig nivå för skyddet av fysiska personer och det fria flödet av personuppgifter inom hela unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens omfattning eller verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen (EU-fördraget). I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.

(171) Direktiv 95/46/EG bör upphävas genom denna förordning. Behandling som redan pågår den dag då denna förordning börjar tillämpas bör bringas i överensstämmelse med denna förordning inom en period av två år från det att denna förordning träder i kraft. Om behandlingen grundar sig på samtycke enligt direktiv 95/46/EG, är det inte nödvändigt att den registrerade på nytt ger sitt samtycke för att den personuppgiftsansvarige ska kunna fortsätta med behandlingen i fråga efter det att denna förordning börjar tillämpas, om det sätt på vilket samtycket gavs överensstämmer med villkoren i denna förordning. Beslut av kommissionen som antagits och tillstånd från tillsynsmyndigheterna som utfärdats på grundval av direktiv 95/46/EG ska fortsatt vara giltiga tills de ändras, ersätts eller upphävs.

(172) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i förordning (EG) nr 45/2001 och avgav ett yttrande den 7 mars 2012 ([1]).

(173) Denna förordning bör vara tillämplig på alla frågor som gäller skyddet av grundläggande rättigheter och friheter i förhållande till behandlingen av personuppgifter, vilka inte omfattas av särskilda skyldigheter med samma mål som anges i Europaparlamentets och rådets direktiv 2002/58/EG ([2]), däribland den personuppgiftsansvariges skyldigheter och fysiska personers rättigheter. För att klargöra förhållandet mellan denna förordning och direktiv 2002/58/EG bör det direktivet ändras. När denna förordning har antagits, bör direktiv 2002/58/EG ses över, framför allt för att säkerställa konsekvens med denna förordning.

([1]) EUT C 192, 30.6.2012, s. 7.

([2]) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Allmänna bestämmelser

Artikel 1

Syfte

1. I denna förordning fastställs bestämmelser om skydd för fysiska personer med avseende på behandlingen av personuppgifter och om det fria flödet av personuppgifter.

2. Denna förordning skyddar fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.

3. Det fria flödet av personuppgifter inom unionen får varken begränsas eller förbjudas av skäl som rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter.

Artikel 2

Materiellt tillämpningsområde

1. Denna förordning ska tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.

2. Denna förordning ska inte tillämpas på behandling av personuppgifter som

a) utgör ett led i en verksamhet som inte omfattas av unionsrätten,

b) medlemsstaterna utför när de bedriver verksamhet som omfattas av avdelning V kapitel 2 i EU-fördraget,

c) en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll,

d) behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

3. Förordning (EG) nr 45/2001 är tillämplig på den behandling av personuppgifter som sker i EU:s institutioner, organ och byråer. Förordning (EG) nr 45/2001 och de av unionens övriga rättsakter som är tillämpliga på sådan behandling av personuppgifter ska anpassas till principerna och bestämmelserna i denna förordning i enlighet med artikel 98.

4. Denna förordning påverkar inte tillämpningen av direktiv 2000/31/EG, särskilt bestämmelserna om tjänsteleverera nde mellanhänders ansvar i artiklarna 12–15 i det direktivet.

Artikel 3

Territoriellt tillämpningsområde

1. Denna förordning ska tillämpas på behandlingen av personuppgifter inom ramen för den verksamhet som bedrivs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad i unionen, oavsett om behandlingen utförs i unionen eller inte.

2. Denna förordning ska tillämpas på behandling av personuppgifter som avser registrerade som befinner sig i unionen och som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad i unionen, om behandlingen har anknytning till

a) utbjudande 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 identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift 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 personuppgiftsbiträdets direkta ansvar är behöriga att behandla personuppgifterna,

11. *samtycke* 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 personuppgiftsbiträdets verksamhetsställen i unionen där den huvudsakliga behandlingen inom ramen för verksamheten vid ett av personuppgiftsbiträdets 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

    a) den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad på tillsynsmyndighetens medlemsstats territorium,

    b) registrerade som är bosatta i den tillsynsmyndighetens medlemsstat i väsentlig grad påverkas eller sannolikt i väsentlig grad kommer att påverkas av behandlingen, eller

    c) ett klagomål har lämnats in till denna tillsynsmyndighet,

23. *gränsöverskridande behandling*:

    a) 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

    b) behandling av personuppgifter som äger rum inom ramen för verksamhet vid ett enda verksamhetsställe tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen men som i väsentlig grad påverkar eller sannolikt i väsentlig grad kommer att påverka registrerade i mer än en medlemsstat,

24. *relevant och motiverad invändning*: en invändning mot ett förslag till beslut avseende frågan huruvida det föreligger en överträdelse av denna förordning eller huruvida den planerade åtgärden i förhållande till den personuppgiftsansvarige eller personuppgiftsbiträdet är förenlig med denna förordning, av vilken invändning det tydligt framgår hur stora risker utkastet till beslut medför när det gäller registrerades grundläggande rättigheter och friheter samt i tillämpliga fall det fria flödet av personuppgifter inom unionen,

25. *informationssamhällets tjänster*: alla tjänster enligt definitionen i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535 ([1]),

26. *internationell organisation*: en organisation och dess underställda organ som lyder under folkrätten, eller ett annat organ som inrättats genom eller på grundval av en överenskommelse mellan två eller flera länder.

KAPITEL II

Principer

Artikel 5

Principer för behandling av personuppgifter

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 oförenlig 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*).

([1]) Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (EUT L 241, 17.9.2015, s. 1).

e) De får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, under förutsättning att de lämpliga tekniska och organisatoriska åtgärder som krävs enligt denna förordning genomförs för att säkerställa den registrerades rättigheter och friheter (*lagringsminimering*).

f) De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring 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 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.

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 föräldraansvar för barnet.

Medlemsstaterna får i sin nationella rätt föreskriva en lägre ålder i detta syfte, under förutsättning att denna lägre ålder inte är under 13 år.

2. Den personuppgiftsansvarige ska göra rimliga ansträngningar för att i sådana fall kontrollera att samtycke ges eller godkänns av den person som har föräldraansvar för barnet, med hänsyn tagen till tillgänglig teknik.

3. Punkt 1 ska inte påverka tillämpningen av allmän avtalsrätt i medlemsstaterna, såsom bestämmelser om giltigheten, upprättandet eller effekten av ett avtal som gäller ett barn.

Artikel 9

Behandling av särskilda kategorier av personuppgifter

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

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

a) Den registrerade har uttryckligen lämnat sitt samtycke till behandlingen av dessa personuppgifter för ett eller flera specifika ändamål, utom då unionsrätten eller medlemsstaternas nationella rätt föreskriver att förbudet i punkt 1 inte kan upphävas av den registrerade.

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

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

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

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

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

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

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

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

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

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

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

Artikel 10

Behandling av personuppgifter som rör fällande domar i brottmål samt överträdelser

Behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder enligt artikel 6.1 får endast utföras under kontroll av myndighet eller då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs. Ett fullständigt register över fällande domar i brottmål får endast föras under kontroll av en myndighet.

Artikel 11

Behandling som inte kräver identifiering

1. Om de ändamål för vilka den personuppgiftsansvarige behandlar personuppgifter inte kräver eller inte längre kräver att den registrerade identifieras av den personuppgiftsansvarige, ska den personuppgiftsansvarige inte vara tvungen att bevara, förvärva eller behandla ytterligare information för att identifiera den registrerade endast i syfte att följa denna förordning.

2. Om den personuppgiftsansvarige, i de fall som avses i punkt 1 i denna artikel, kan visa att denne inte är i stånd att identifiera den registrerade, ska den personuppgiftsansvarige om möjligt informera den registrerade om detta. I sådana fall ska artiklarna 15–20 inte gälla, förutom när den registrerade för utövande av sina rättigheter i enlighet med dessa artiklar tillhandahåller ytterligare information som gör identifieringen möjlig.

KAPITEL III

Den registrerades rättigheter

Avsnitt 1

Insyn och villkor

Artikel 12

Klar och tydlig information och kommunikation samt klara och tydliga villkor för utövandet av den registrerades rättigheter

1. Den personuppgiftsansvarige ska vidta lämpliga åtgärder för att till den registrerade tillhandahålla all information som avses i artiklarna 13 och 14 och all kommunikation enligt artiklarna 15–22 och 34 vilken avser behandling i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, i synnerhet för information som är särskilt riktad till barn. Informationen ska tillhandahållas skriftligt, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form. Om den registrerade begär det får informationen tillhandahållas muntligt, förutsatt att den registrerades identitet bevisats på andra sätt.

2. Den personuppgiftsansvarige ska underlätta utövandet av den registrerades rättigheter i enlighet med artiklarna 15–22. I de fall som avses i artikel 11.2 får den personuppgiftsansvarige inte vägra att tillmötesgå den registrerades begäran om att utöva sina rättigheter enligt artiklarna 15–22, om inte den personuppgiftsansvarige visar att han eller hon inte är i stånd att identifiera den registrerade.

3. Den personuppgiftsansvarige ska på begäran utan onödigt dröjsmål och under alla omständigheter senast en månad efter att ha mottagit begäran tillhandahålla den registrerade information om de åtgärder som vidtagits enligt artiklarna 15–22. Denna period får vid behov förlängas med ytterligare två månader, med beaktande av hur komplicerad begäran är och antalet inkomna begäranden. Den personuppgiftsansvarige ska underrätta den registrerade om en sådan förlängning inom en månad från det att begäran mottagits samt ange orsakerna till förseningen. Om den registrerade lämnar begäran i elektronisk form, ska informationen om möjligt tillhandahållas i elektronisk form, om den registrerade inte begär något annat.

4. Om den personuppgiftsansvarige inte vidtar åtgärder på den registrerades begäran, ska den personuppgiftsansvarige utan dröjsmål och senast en månad efter att ha mottagit begäran informera den registrerade om orsaken till att åtgärder inte vidtagits och om möjligheten att lämna in ett klagomål till en tillsynsmyndighet och begära rättslig prövning.

5. Information som tillhandahållits enligt artiklarna 13 och 14, all kommunikation och samtliga åtgärder som vidtas enligt artiklarna 15–22 och 34 ska tillhandahållas kostnadsfritt. Om begäranden från en registrerad är uppenbart ogrundade eller orimliga, särskilt på grund av deras repetitiva art, får den personuppgiftsansvarige antingen

a) ta ut en rimlig avgift som täcker de administrativa kostnaderna för att tillhandahålla den information eller vidta den åtgärd som begärts, eller

b) vägra att tillmötesgå begäran.

Det åligger den personuppgiftsansvarige att visa att begäran är uppenbart ogrundad eller orimlig.

6. Utan att det påverkar tillämpningen av artikel 11 får den personuppgiftsansvarige, om denne har rimliga skäl att betvivla identiteten hos den fysiska person som lämnar in en begäran enligt artiklarna 15–21, begära att ytterligare information som är nödvändig för att bekräfta den registrerades identitet tillhandahålls.

7. Den information som ska tillhandahållas de registrerade i enlighet med artiklarna 13 och 14 får tillhandahållas kombinerad med standardiserade symboler för att ge en överskådlig, begriplig, lättläst och meningsfull överblick över den planerade behandlingen. Om sådana symboler visas elektroniskt ska de vara maskinläsbara.

8. Kommissionen ska ges befogenhet att anta delegerade akter i enlighet med artikel 92 för att fastställa vilken information som ska visas med hjälp av symboler och förfaranden för att tillhandahålla sådana symboler.

Avsnitt 2

Information och tillgång till personuppgifter

Artikel 13

Information som ska tillhandahållas om personuppgifterna samlas in från den registrerade

1. Om personuppgifter som rör en registrerad person samlas in från den registrerade, ska den personuppgiftsansvarige, när personuppgifterna erhålls, till den registrerade lämna information om följande:

a) Identitet och kontaktuppgifter för den personuppgiftsansvarige och i tillämpliga fall för dennes företrädare.

b) Kontaktuppgifter för dataskyddsombudet, i tillämpliga fall.

c) Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen.

d) Om behandlingen är baserad på artikel 6.1 f, den personuppgiftsansvariges eller en tredje parts berättigade intressen.

e) Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall.

f) I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artikel 46, 47 eller artikel 49.1 andra stycket, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.

2. Utöver den information som avses i punkt 1 ska den personuppgiftsansvarige vid insamlingen av personuppgifterna lämna den registrerade följande ytterligare information, vilken krävs för att säkerställa rättvis och transparent behandling:

a) Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.

b) Att det föreligger en rätt att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller att invända mot behandling samt rätten till dataportabilitet.

c) Om behandlingen grundar sig på artikel 6.1 a eller artikel 9.2 a, att det föreligger en rätt att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.

d) Rätten att inge klagomål till en tillsynsmyndighet.

e) Huruvida tillhandahållandet av personuppgifter är ett lagstadgat eller avtalsenligt krav eller ett krav som är nödvändigt för att ingå ett avtal samt huruvida den registrerade är skyldig att tillhandahålla personuppgifterna och de möjliga följderna av att sådana uppgifter inte lämnas.

f) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.

3. Om den personuppgiftsansvarige avser att ytterligare behandla personuppgifterna för ett annat syfte än det för vilket de insamlades, ska den personuppgiftsansvarige före denna ytterligare behandling ge den registrerade information om detta andra syfte samt ytterligare relevant information enligt punkt 2.

4. Punkterna 1, 2 och 3 ska inte tillämpas om och i den mån den registrerade redan förfogar över informationen.

Artikel 14

Information som ska tillhandahållas om personuppgifterna inte har erhållits från den registrerade

1. Om personuppgifterna inte har erhållits från den registrerade, ska den personuppgiftsansvarige förse den registrerade med följande information:

a) Identitet och kontaktuppgifter för den personuppgiftsansvarige och i tillämpliga fall för dennes företrädare.

b) Kontaktuppgifter för dataskyddsombudet, i tillämpliga fall.

c) Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen.

d) De kategorier av personuppgifter som behandlingen gäller.

e) Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall.

f) I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till en mottagare i ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artiklarna 46, 47 eller artikel 49.1 andra stycket, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.

2. Utöver den information som avses i punkt 1 ska den personuppgiftsansvarige lämna den registrerade följande information, vilken krävs för att säkerställa rättvis och transparent behandling när det gäller den registrerade:

a) Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.

b) Om behandlingen grundar sig på artikel 6.1 f, den personuppgiftsansvariges eller en tredje parts berättigade intressen.

c) Förekomsten av rätten att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade och att invända mot behandling samt rätten till dataportabilitet.

d) Om behandlingen grundar sig på artikel 6.1 a eller artikel 9.2 a, rätten att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.

e) Rätten att inge klagomål till en tillsynsmyndighet.

f) Varifrån personuppgifterna kommer och i förekommande fall huruvida de har sitt ursprung i allmänt tillgängliga källor.

g) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.

3. Den personuppgiftsansvarige ska lämna den information som anges i punkterna 1 och 2

a) inom en rimlig period efter det att personuppgifterna har erhållits, dock senast inom en månad, med beaktande av de särskilda omständigheter under vilka personuppgifterna behandlas,

b) om personuppgifterna ska användas för kommunikation med den registrerade, senast vid tidpunkten för den första kommunikationen med den registrerade, eller

c) om ett utlämnande till en annan mottagare förutses, senast när personuppgifterna lämnas ut för första gången.

4. Om den personuppgiftsansvarige avser att ytterligare behandla personuppgifterna för ett annat syfte än det för vilket de insamlades, ska den personuppgiftsansvarige före denna ytterligare behandling ge den registrerade information om detta andra syfte samt ytterligare relevant information enligt punkt 2.

5. Punkterna 1–4 ska inte tillämpas i följande fall och i den mån

a) den registrerade redan förfogar över informationen,

b) tillhandahållandet av sådan information visar sig vara omöjligt eller skulle medföra en oproportionell ansträngning, särskilt för behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, eller i den mån den skyldighet som avses i punkt 1 i den här artikeln sannolikt kommer att göra det omöjligt eller avsevärt försvårar uppfyllandet av målen med den behandlingen; i sådana fall ska den personuppgiftsansvarige vidta lämpliga åtgärder för att skydda den registrerades rättigheter och friheter och berättigade intressen, inbegripet göra uppgifterna tillgängliga för allmänheten,

c) erhållande eller utlämnande av uppgifter uttryckligen föreskrivs genom unionsrätten eller genom en medlemsstats nationella rätt som den registrerade omfattas av och som fastställer lämpliga åtgärder för att skydda den registrerades berättigade intressen, eller

d) personuppgifterna måste förbli konfidentiella till följd av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt, inbegripet andra lagstadgade sekretessförpliktelser.

Artikel 15

Den registrerades rätt till tillgång

1. Den registrerade ska ha rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna och följande information:

a) Ändamålen med behandlingen.

b) De kategorier av personuppgifter som behandlingen gäller.

c) De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, särskilt mottagare i tredjeländer eller internationella organisationer.

d) Om möjligt, den förutsedda period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.

e) Förekomsten av rätten att av den personuppgiftsansvarige begära rättelse eller radering av personuppgifterna eller 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 försvårar uppnåendet av syftet med den behandlingen.

e) För att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

Artikel 18

Rätt till begränsning av behandling

1. Den registrerade ska ha rätt att av den personuppgiftsansvarige kräva att behandlingen begränsas om något av följande alternativ är tillämpligt:

a) Den registrerade bestrider personuppgifternas korrekthet, under en tid som ger den personuppgiftsansvarige möjlighet att kontrollera om personuppgifterna är korrekta.

b) Behandlingen är olaglig och den registrerade motsätter sig att personuppgifterna raderas och i stället begär en begränsning av deras användning.

c) Den personuppgiftsansvarige behöver inte längre personuppgifterna för ändamålen med behandlingen men den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

d) Den registrerade har invänt mot behandling i enlighet med artikel 21.1 i väntan på kontroll av huruvida den personuppgiftsansvariges berättigade skäl väger tyngre än den registrerades berättigade skäl.

2. Om behandlingen har begränsats i enlighet med punkt 1 får sådana personuppgifter, med undantag för lagring, endast behandlas med den registrerades samtycke eller för att fastställa, göra gällande eller försvara rättsliga anspråk eller för att skydda någon annan fysisk eller juridisk persons rättigheter eller för skäl som rör ett viktigt allmänintresse för unionen eller för en medlemsstat.

3. En registrerad som har fått behandling begränsad i enlighet med punkt 1 ska underrättas av den personuppgiftsansvarige innan begränsningen av behandlingen upphör.

Artikel 19

Anmälningsskyldighet avseende rättelse eller radering av personuppgifter och begränsning av behandling

Den personuppgiftsansvarige ska underrätta varje mottagare till vilken personuppgifterna har lämnats ut om eventuella rättelser eller radering av personuppgifter eller begränsningar av behandling som skett i enlighet med artiklarna 16, 17.1 och 18, om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Den personuppgiftsansvarige ska informera den registrerade om dessa mottagare på den registrerades begäran.

Artikel 20

Rätt till dataportabilitet

1. Den registrerade ska ha rätt att få ut de personuppgifter som rör honom eller henne och som han eller hon har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format och ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan att den personuppgiftsansvarige som tillhandahållits personuppgifterna hindrar detta, om

a) behandlingen grundar sig på samtycke enligt artikel 6.1 a eller artikel 9.2 a eller på ett avtal enligt artikel 6.1 b, och

b) behandlingen sker automatiserat.

2 Vid utövandet av sin rätt till dataportabilitet i enlighet med punkt 1 ska den registrerade ha rätt till överföring av personuppgifterna direkt från en personuppgiftsansvarig till en annan, när detta är tekniskt möjligt.

3. Utövandet av den rätt som avses i punkt 1 i den här artikeln ska inte påverka tillämpningen av artikel 17. Den rätten ska inte gälla i fråga om en behandling som är nödvändig för att utföra en uppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den personuppgiftsansvarige.

4. Den rätt som avses i punkt 1 får inte påverka andras rättigheter och friheter på ett ogynnsamt sätt.

Avsnitt 4

Rätt att göra invändningar och automatiserat individuellt beslutsfattande

Artikel 21

Rätt att göra invändningar

1. Den registrerade ska, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att när som helst göra invändningar mot behandling av personuppgifter avseende honom eller henne som grundar sig på artikel 6.1 e eller f, inbegripet profilering som grundar sig på dessa bestämmelser. Den personuppgiftsansvarige får inte längre behandla personuppgifterna såvida denne inte kan påvisa tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk.

2. Om personuppgifterna behandlas för direkt marknadsföring ska den registrerade ha rätt att när som helst invända mot behandling av personuppgifter som avser honom eller henne för sådan marknadsföring, vilket inkluderar profilering i den utsträckning som denna har ett samband med sådan direkt marknadsföring.

3. Om den registrerade invänder mot behandling för direkt marknadsföring ska personuppgifterna inte längre behandlas för sådana ändamål.

4. Senast vid den första kommunikationen med den registrerade ska den rätt som avses i punkterna 1 och 2 uttryckligen meddelas den registrerade och redovisas tydligt, klart och åtskilt från eventuell annan information.

5. När det gäller användningen av informationssamhällets tjänster, och trots vad som sägs i direktiv 2002/58/EG, får den registrerade utöva sin rätt att göra invändningar på automatiserat sätt med användning av tekniska specifikationer.

6. Om personuppgifter behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska den registrerade, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att göra invändningar mot behandling av personuppgifter avseende honom eller henne om inte behandlingen är nödvändig för att utföra en uppgift av allmänt intresse.

Artikel 22

Automatiserat individuellt beslutsfattande, inbegripet profilering

1. Den registrerade ska ha rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne.

2. Punkt 1 ska inte tillämpas om beslutet

a) är nödvändigt för ingående eller fullgörande av ett avtal mellan den registrerade och den personuppgiftsansvarige,

b) tillåts enligt unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av och som fastställer lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen, eller

c) grundar sig på den registrerades uttryckliga samtycke.

3. I fall som avses i punkt 2 a och c ska den personuppgiftsansvarige genomföra lämpliga åtgärder för att säkerställa den registrerades rättigheter, friheter och rättsliga intressen, åtminstone rätten till personlig kontakt med den personuppgiftsansvarige för att kunna utrycka sin åsikt och bestrida beslutet.

4. Beslut enligt punkt 2 får inte grunda sig på de särskilda kategorier av personuppgifter som avses i artikel 9.1, såvida inte artikel 9.2 a eller g gäller och lämpliga åtgärder som ska skydda den registrerades berättigade intressen har vidtagits.

Avsnitt 5

Begränsningar

Artikel 23

Begränsningar

1. Det ska vara möjligt att i unionsrätten eller i en medlemsstats nationella rätt som den personuppgiftsansvarige eller personuppgiftsbiträdet omfattas av införa en lagstiftningsåtgärd som begränsar tillämpningsområdet för de skyldigheter och rättigheter som föreskrivs i artiklarna 12–22 och 34, samt artikel 5 i den mån dess bestämmelser motsvarar de rättigheter och skyldigheter som fastställs i artiklarna 12–22, om en sådan begränsning sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa

a) den nationella säkerheten,

b) försvaret,

c) den allmänna säkerheten,

d) förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten,

e) andra av unionens eller en medlemsstats viktiga mål av generellt allmänt intresse, särskilt ett av unionens eller en medlemsstats viktiga ekonomiska eller finansiella intressen, däribland penning-, budget- eller skattefrågor, folkhälsa och social trygghet,

f) skydd av rättsväsendets oberoende och rättsliga åtgärder,

g) förebyggande, förhindrande, utredning, avslöjande och lagföring av överträdelser av etiska regler som gäller för lagreglerade yrken,

h) en tillsyns-, inspektions- eller regleringsfunktion som, även i enstaka fall, har samband med myndighetsutövning i fall som nämns i a–e och g,

i) skydd av den registrerade eller andras rättigheter och friheter,

j) verkställighet av civilrättsliga krav.

2. Framför allt ska alla lagstiftningsåtgärder som avses i punkt 1 innehålla specifika bestämmelser åtminstone, när så är relevant, avseende

a) ändamålen med behandlingen eller kategorierna av behandling,

b) kategorierna av personuppgifter,

c) omfattningen av de införda begränsningarna,

d) skyddsåtgärder för att förhindra missbruk eller olaglig tillgång eller överföring,

e) specificeringen av den personuppgiftsansvarige eller kategorierna av personuppgiftsansvariga,

f) lagringstiden samt tillämpliga skyddsåtgärder med beaktande av behandlingens art, omfattning och ändamål eller kategorierna av behandling,

g) riskerna för de registrerades rättigheter och friheter, och

h) de registrerades rätt att bli informerade om begränsningen, såvida detta inte kan inverka menligt på begränsningen.

KAPITEL IV

Personuppgiftsansvarig och personuppgiftsbiträde

Avsnitt 1

Allmänna skyldigheter

Artikel 24

Den personuppgiftsansvariges ansvar

1. Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning. Dessa åtgärder ska ses över och uppdateras vid behov.

2. Om det står i proportion till behandlingen, ska de åtgärder som avses i punkt 1 omfatta den personuppgiftsansvariges genomförande av lämpliga strategier för dataskydd.

3. Tillämpningen av godkända uppförandekoder som avses i artikel 40 eller godkända certifieringsmekanismer som avses i artikel 42 får användas för att visa att den personuppgiftsansvarige fullgör sina skyldigheter.

Artikel 25

Inbyggt dataskydd och dataskydd som standard

1. Med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige, både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder – såsom pseudonymisering – vilka är utformade för ett effektivt genomförande av dataskyddsprinciper – såsom uppgiftsminimering – och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, så att kraven i denna förordning uppfylls och den registrerades rättigheter skyddas.

2. Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.

3. En godkänd certifieringsmekanism i enlighet med artikel 42 får användas för att visa att kraven i punkterna 1 och 2 i den här artikeln följs.

Artikel 26

Gemensamt personuppgiftsansvariga

1. Om två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga. Gemensamt personuppgiftsansvariga ska under öppna former fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt denna förordning, särskilt vad gäller utövandet av den registrerades rättigheter och sina respektive skyldigheter att tillhandahålla den information som avses i artiklarna 13 och 14, genom ett inbördes arrangemang, såvida inte de personuppgiftsansvarigas respektive skyldigheter fastställs genom unionsrätten eller en medlemsstats nationella rätt som de personuppgiftsansvariga omfattas av. Inom ramen för arrangemanget får en gemensam kontaktpunkt för de personuppgiftsansvariga utses.

2. Det arrangemang som avses i punkt 1 ska på lämpligt sätt återspegla de gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot registrerade. Det väsentliga innehållet i arrangemanget ska göras tillgängligt för den registrerade.

3. Oavsett formerna för det arrangemang som avses i punkt 1 får den registrerade utöva sina rättigheter enligt denna förordning med avseende på och emot var och en av de personuppgiftsansvariga.

Artikel 27

Företrädare för personuppgiftsansvariga eller personuppgiftsbiträden som inte är etablerade i unionen

1. Om artikel 3.2 tillämpas ska den personuppgiftsansvarige eller personuppgiftsbiträdet skriftligen utse en företrädare i unionen.

2. Skyldigheten enligt punkt 1 i denna artikel ska inte gälla

a) tillfällig behandling som inte omfattar behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1, eller behandling av personuppgifter avseende fällande domar i brottmål samt 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 personuppgiftsbiträdets 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 förhandstillstånd 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 anlitandet av ett annat personuppgiftsbiträde,

e) med tanke på behandlingens art, ska hjälpa den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att den personuppgiftsansvarige kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter i enlighet med kapitel III,

f) ska bistå den personuppgiftsansvarige med att se till att skyldigheterna enligt artiklarna 32–36 fullgörs, med beaktande av typen av behandling och den information som 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 utförts under dess ansvar. Detta register ska innehålla samtliga följande uppgifter:

a) Namn och kontaktuppgifter för den personuppgiftsansvarige, samt i tillämpliga fall gemensamt personuppgiftsansvariga, den personuppgiftsansvariges företrädare samt dataskyddsombudet.

b) Ändamålen med behandlingen.

c) En beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter.

d) De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, inbegripet mottagare i tredjeländer eller i internationella organisationer.

e) I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och, vid sådana överföringar som avses i artikel 49.1 andra stycket, dokumentationen av lämpliga skyddsåtgärder.

f) Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.

g) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1.

2. Varje personuppgiftsbiträde och, i tillämpliga fall, dennes företrädare ska föra ett register över alla kategorier av behandling som utförts för den personuppgiftsansvariges räkning, som omfattar följande:

a) Namn och kontaktuppgifter för personuppgiftsbiträdet eller personuppgiftsbiträdena och för varje personuppgiftsansvarig för vars räkning personuppgiftsbiträdet agerar, och, i tillämpliga fall, för den personuppgiftsansvariges eller 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 tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och, vid sådana överföringar som avses i artikel 49.1 andra stycket, dokumentationen av lämpliga skyddsåtgärder.

d) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1.

3. De register som avses i punkterna 1 och 2 ska upprättas skriftligen, inbegripet i elektronisk form.

4. På begäran ska den personuppgiftsansvarige eller personuppgiftsbiträdet samt, i tillämpliga fall, den personuppgiftsansvariges eller 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 överträdelser som avses i artikel 10.

Artikel 31

Samarbete med tillsynsmyndigheten

Den personuppgiftsansvarige och personuppgiftsbiträdet samt, i tillämpliga fall, deras företrädare ska på begäran samarbeta med tillsynsmyndigheten vid utförandet av dennes uppgifter.

Avsnitt 2

Säkerhet för personuppgifter

Artikel 32

Säkerhet i samband med behandlingen

1. Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt

a) pseudonymisering och kryptering av personuppgifter,

b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,

c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,

d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

2. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

3. Anslutning till en godkänd uppförandekod som avses i artikel 40 eller en godkänd certifieringsmekanism som avses i artikel 42 får användas för att visa att kraven i punkt 1 i den här artikeln följs.

4. Den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets 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 överträdelser 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 personuppgiftsbiträdets 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 personuppgiftsbiträdets 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 överträdelser, som avses i artikel 10.

2. En koncern får utnämna ett enda dataskyddsombud om det på varje etableringsort är lätt att nå ett dataskyddsombud.

3. Om den personuppgiftsansvarige eller personuppgiftsbiträdet är en myndighet eller ett offentligt organ, får ett enda dataskyddsombud utnämnas för flera sådana myndigheter eller organ, med hänsyn till deras organisationsstruktur och storlek.

4. I andra fall än de som avses i punkt 1 får eller, om så krävs enligt unionsrätten eller medlemsstaternas nationella rätt, ska den personuppgiftsansvarige eller personuppgiftsbiträdet eller sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden utnämna ett dataskyddsombud. Dataskyddsombudet får agera för sådana sammanslutningar och andra organ som företräder personuppgiftsansvariga eller personuppgiftsbiträden.

5. Dataskyddsombudet ska utses på grundval av yrkesmässiga kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som avses i artikel 39.

6. Dataskyddsombudet får ingå i den personuppgiftsansvariges eller personuppgiftsbiträdets 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 uppgiftskyddsombudet 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 personuppgiftsbiträdets högsta förvaltningsnivå.

4. Den registrerade får kontakta dataskyddsombudet med avseende på alla frågor som rör behandlingen av dennes personuppgifter och utövandet 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 personuppgiftsbiträdets strategi för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.

c) Att på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den enligt artikel 35.

d) Att samarbeta med tillsynsmyndigheten.

e) Att fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling, inbegripet det förhandssamråd som avses i artikel 36, och vid behov samråda i alla andra frågor.

2. 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 föräldraansvar 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 det 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 samla alla godkända uppförandekoder, ändringar och utökningar i ett register och offentliggöra dem på lämpligt sätt.

Artikel 41

Övervakning av godkända uppförandekoder

1. Utan att det påverkar den berörda tillsynsmyndighetens uppgifter och befogenheter enligt artiklarna 57 och 58 får övervakningen av efterlevnaden av en uppförandekod i enlighet med artikel 40 utföras av ett organ som har en lämplig expertnivå i förhållande till kodens syfte och som ackrediteras för detta ändamål av den behöriga tillsynsmyndigheten.

2. Ett organ som avses i punkt 1 får ackrediteras för att övervaka efterlevnaden av en uppförandekod om detta organ har

a) visat sitt oberoende och sin expertis i förhållande till uppförandekodens syfte på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande,

b) upprättat förfaranden varigenom det kan bedöma de berörda personuppgiftsansvarigas och personuppgiftsbiträdenas lämplighet för att tillämpa uppförandekoden, övervaka att de efterlever dess bestämmelser och regelbundet se över hur den fungerar,

c) upprättat förfaranden och strukturer för att hantera klagomål om överträdelser av uppförandekoden eller det sätt på vilket uppförandekoden har tillämpats, eller tillämpas, av en personuppgiftsansvarig eller ett personuppgiftsbiträde, och för att göra dessa förfaranden och strukturer synliga för registrerade och för allmänheten, och

d) på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande visat att dess uppgifter och uppdrag inte leder till en intressekonflikt.

3. Den behöriga tillsynsmyndigheten ska inlämna utkastet till kriterier för ackreditering av ett organ som avses i punkt 1 i den här artikeln till styrelsen i enlighet med den mekanism för enhetlighet som avses i artikel 63.

4. Utan att det påverkar den behöriga tillsynsmyndighetens uppgifter och befogenheter och tillämpningen av bestämmelserna i kapitel VIII ska ett organ som avses i punkt 1 i denna artikel, med förbehåll för tillräckliga skyddsåtgärder, vidta lämpliga åtgärder i fall av en personuppgiftsansvarigs eller ett personuppgiftsbiträdes överträdelse av uppförandekoden, inbegripet avstängning eller uteslutande av den personuppgiftsansvarige eller personuppgiftsbiträdet från uppförandekoden. Det ska informera den behöriga tillsynsmyndigheten om sådana åtgärder och skälen för att de vidtagits.

5. Den behöriga tillsynsmyndigheten ska återkalla ackrediteringen av ett organ som avses i punkt 1 om villkoren för ackrediteringen inte, eller inte längre, uppfylls eller om åtgärder som vidtagits av organet strider mot denna förordning.

6. Denna artikel ska inte gälla behandling som utförs av offentliga myndigheter och organ.

Artikel 42

Certifiering

1. Medlemsstaterna, tillsynsmyndigheterna, styrelsen och kommissionen ska uppmuntra, särskilt på unionsnivå, införandet av certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd som syftar till att visa att personuppgiftsansvarigas eller personuppgiftsbiträdens behandling är förenlig med denna förordning. De särskilda behoven hos mikroföretag samt små och medelstora företag ska beaktas.

2. Certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd som är godkända enligt punkt 5 i denna artikel får, förutom att de iakttas av personuppgiftsansvariga eller personuppgiftsbiträden som omfattas av denna förordning, inrättas för att visa att det föreligger lämpliga garantier som tillhandahålls av personuppgiftsansvariga och personuppgiftsbiträden som inte omfattas av denna förordning enligt artikel 3, inom ramen för överföringar av personuppgifter till tredjeländer eller internationella organisationer enligt villkoren i artikel 46.2 f. Sådana personuppgiftsansvariga eller personuppgiftsbiträden ska göra bindande och verkställbara åtaganden, genom avtal eller andra rättsligt bindande instrument, att tillämpa dessa lämpliga garantier, inbegripet när det gäller registrerades rättigheter.

3. Certifieringen ska vara frivillig och tillgänglig via ett öppet förfarande.

4. En certifiering i enlighet med denna artikel minskar inte den personuppgiftsansvariges eller 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 ([1]) i enlighet med EN-ISO/IEC 17065/2012 och med de ytterligare krav som fastställts av den tillsynsmyndighet som är behörig enligt artikel 55 eller 56.

2. Certifieringsorgan som avses i punkt 1 får ackrediteras i enlighet med den punkten endast om de har

a) visat oberoende och expertis i förhållande till certifieringens syfte på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande,

([1]) Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30).

b) förbundit sig att respektera de kriterier som avses i artikel 42.5 och godkänts av den tillsynsmyndighet som är behörig enligt artikel 55 eller 56, eller av styrelsen enligt artikel 63,

c) upprättat förfaranden för utfärdande, periodisk översyn och återkallande av certifiering, sigill och märkningar för dataskydd,

d) upprättat förfaranden och strukturer för att hantera klagomål om överträdelser av certifieringen eller det sätt på vilket certifieringen har tillämpats, eller tillämpas, av en personuppgiftsansvarig eller ett personuppgiftsbiträde, och för att göra dessa förfaranden och strukturer synliga för registrerade och för allmänheten, och

e) på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande visat att deras uppgifter och uppdrag inte leder till en intressekonflikt.

3. Ackrediteringen av certifieringsorgan som avses i punkterna 1 och 2 i denna artikel ska ske på grundval av kriterier som godkänts av den tillsynsmyndighet som är behörig enligt artikel 55 eller 56, eller av styrelsen enligt artikel 63. I händelse av ackreditering enligt punkt 1 b i den här artikeln ska dessa krav komplettera dem som föreskrivs i förordning (EG) nr 765/2008 och de tekniska regler som beskriver certifieringsorganens metoder och förfaranden.

4. De certifieringsorgan som avses i punkt 1 ska ansvara för den korrekta bedömning som leder till certifieringen eller återkallelsen av certifieringen, utan att det påverkar den personuppgiftsansvariges eller personuppgiftsbiträdets 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 överförts till ett tredjeland eller en internationell organisation får bara ske under förutsättning att den personuppgiftsansvarige och personuppgiftsbiträdet, med förbehåll för övriga bestämmelser i denna förordning, uppfyller villkoren i detta kapitel, inklusive för vidare överföring av personuppgifter från tredjelandet eller den internationella organisationen till ett annat tredjeland eller en annan internationell organisation. Alla bestämmelser i detta kapitel ska tillämpas för att säkerställa att den nivå på skyddet av fysiska personer som säkerställs genom denna förordning inte undergrävs.

Artikel 45

Överföring på grundval av ett beslut om adekvat skyddsnivå

1. Personuppgifter får överföras till ett tredjeland eller en internationell organisation om kommissionen har beslutat att tredjelandet, ett territorium eller en eller flera specificerade sektorer i tredjelandet, eller den internationella organisationen i fråga säkerställer en adekvat skyddsnivå. En sådan överföring ska inte kräva något särskilt tillstånd.

2. När kommissionen bedömer om en adekvat skyddsnivå föreligger ska den särskilt beakta

a) rättsstatsprincipen, respekten för de mänskliga rättigheterna och de grundläggande friheterna, relevant lagstiftning, både allmän lagstiftning och sektorslagstiftning, inklusive avseende allmän säkerhet, försvar, nationell säkerhet och straffrätt och offentliga myndigheters tillgång till personuppgifter samt tillämpningen av sådan lagstiftning, dataskyddsregler, yrkesregler och säkerhetsbestämmelser, inbegripet regler för vidare överföring av personuppgifter till ett annat tredjeland eller en annan internationell organisation, som ska följas i det landet eller den internationella organisationen, rättspraxis samt faktiska och verkställbara rättigheter för registrerade och effektiv administrativ och rättslig prövning för de registrerade vars personuppgifter överförs,

b) huruvida det finns en eller flera effektivt fungerande oberoende tillsynsmyndigheter i tredjelandet, eller som utövar tillsyn över den internationella organisationen, som har ansvar för att säkerställa och kontrollera att dataskyddsregler följs, inklusive lämpliga verkställighetsbefogenheter, ge de registrerade råd och assistans när det gäller utövandet av deras rättigheter och samarbeta med medlemsstaternas tillsynsmyndigheter, och

c) vilka internationella åtaganden det berörda tredjelandet eller den berörda internationella organisationen har gjort, eller andra skyldigheter som följer av rättsligt bindande konventioner eller instrument samt av dess deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter.

3. Kommissionen får, efter att ha bedömt om det föreligger en adekvat skyddsnivå, genom en genomförandeakt besluta att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom ett tredjeland, eller en internationell organisation säkerställer en adekvat skyddsnivå i den mening som avses i punkt 2 i den här artikeln. Genomförandeakten ska inrätta en mekanism för regelbunden översyn, minst vart fjärde år, som ska beakta all relevant utveckling i det tredjelandet eller den internationella organisationen. Beslutets territoriella och sektorsmässiga tillämpning ska regleras i genomförandeakten, där det också i förekommande fall ska anges vilken eller vilka myndigheter som är tillsynsmyndighet(er) enligt punkt 2 b i den här artikeln. Genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

4. Kommissionen ska fortlöpande övervaka utveckling i tredjeländer och internationella organisationer vilken kan påverka hur beslut som antagits enligt punkt 3 i den här artikeln och beslut som antagits på grundval av artikel 25.6 i direktiv 95/46/EG fungerar.

5. Kommissionen ska, när tillgänglig information visar, i synnerhet efter den översyn som avses i punkt 3 i den här artikeln, att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom tredjelandet i fråga eller en internationell organisation inte längre säkerställer adekvat skydd i den mening som avses i punkt 2 i den här artikeln och, i den mån det behövs, genom genomförandeakter återkalla, ändra eller upphäva det beslut som avses i punkt 3 i den här artikeln utan retroaktiv verkan. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

När det föreligger vederbörligen motiverade och tvingande skäl till skyndsamhet ska kommissionen anta omedelbart tillämpliga genomförandeakter i enlighet med det förfarande som avses i artikel 93.3.

6. Kommissionen ska samråda med tredjelandet eller den internationella organisationen i fråga för att lösa den situation som lett till beslutet enligt punkt 5.

7. Beslut enligt punkt 5 i den här artikeln ska inte påverka överföring av personuppgifter till tredjelandet, ett territorium eller en eller flera specificerade sektorer inom tredjelandet, eller den internationella organisationen i fråga enligt artiklarna 46–49.

8. Kommissionen ska i *Europeiska unionens officiella tidning* och på sin webbplats offentliggöra en förteckning över de tredjeländer och de territorier och specificerade sektorer i ett givet tredjeland samt de internationella organisationer för vilka den har fastställt att en adekvat skyddsnivå inte eller inte längre säkerställs.

9. De beslut som antas av kommissionen på grundval av artikel 25.6 i direktiv 95/46/EG ska förbli i kraft tills de ändrats, ersatts eller upphävts av ett kommissionsbeslut som antagits i enlighet med punkt 3 eller 5 i den här artikeln.

Artikel 46

Överföring som omfattas av lämpliga skyddsåtgärder

1. I avsaknad av ett beslut i enlighet med artikel 45.3, får en personuppgiftsansvarig eller ett personuppgiftsbiträde endast överföra personuppgifter till ett tredjeland eller en internationell organisation efter att ha vidtagit lämpliga skyddsåtgärder, och på villkor att lagstadgade rättigheter för registrerade och effektiva rättsmedel för registrerade finns tillgängliga.

2. Lämpliga skyddsåtgärder enligt punkt 1 får, utan att det krävs särskilt tillstånd från en övervakningsmyndighet, ta formen av

a) ett rättsligt bindande och verkställbart instrument mellan offentliga myndigheter eller organ,

b) bindande företagsbestämmelser i enlighet med artikel 47,

c) standardiserade dataskyddsbestämmelser som antas av kommissionen i enlighet med det granskningsförfarande som avses i artikel 93.2,

d) standardiserade dataskyddsbestämmelser som antagits av en tillsynsmyndighet och godkänts av kommissionen i enlighet med det granskningsförfarande som avses i artikel 93.2,

e) en godkänd uppförandekod enlig 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 enlig artikel 42 tillsammans med rättsligt bindande och verkställbara åtaganden för den personuppgiftsansvarige, personuppgiftsbiträdet i tredjelandet att tillämpa lämpliga skyddsåtgärder, även när det gäller de registrerades rättigheter.

3. Med förbehåll för tillstånd från den behöriga tillsynsmyndigheten, får lämpliga skyddsåtgärder enligt punkt 1 också i synnerhet ta formen av

a) avtalsklausuler mellan den personuppgiftsansvarige eller personuppgiftsbiträdet och den personuppgiftsansvarige, personuppgiftsbiträdet eller mottagaren av personuppgifterna i tredjelandet eller den internationella organisationen, eller

b) bestämmelser som ska införas i administrativa överenskommelser mellan offentliga myndigheter eller organ vilka inbegriper verkställbara och faktiska rättigheter för registrerade.

4. Tillsynsmyndigheten ska tillämpa den mekanism för enhetlighet som avses i artikel 63 i de fall som avses i punkt 3 i den här artikeln.

5. Tillstånd från en medlemsstat eller tillsynsmyndighet på grundval av artikel 26.2 i direktiv 95/46/EG ska förbli giltigt tills det, vid behov, ändrats, ersatts eller upphävts av den tillsynsmyndigheten. De beslut som fattas av kommissionen på grundval av artikel 26.4 i direktiv 95/46/EG ska förbli i kraft tills de, vid behov, ändrats, ersatts eller upphävts av ett kommissionsbeslut som antagits i enlighet med punkt 2 i den här artikeln.

Artikel 47

Bindande företagsbestämmelser

1. Den behöriga tillsynsmyndigheten ska godkänna bindande företagsbestämmelser i enlighet med den mekanism för enhetlighet som föreskrivs i artikel 63 under förutsättning att de

a) är rättslig bindande, tillämpas på, och verkställs av alla delar som berörs inom den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet, inklusive deras anställda,

b) innehåller uttryckliga bestämmelser om de registrerades lagstadgade rättigheter när det gäller behandlingen av deras personuppgifter, och

c) uppfyller villkoren i punkt 2.

2. De bindande företagsbestämmelser som avses i punkt 1 ska närmare ange åtminstone följande:

a) struktur och kontaktuppgifter för den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet och för var och en av dess medlemmar,

b) vilka överföringar eller uppsättningar av överföringar av uppgifter som omfattas, inklusive kategorierna av personuppgifter, typen av behandling och dess ändamål, den typ av registrerade som berörs samt vilket eller vilka tredjeländer som avses,

c) bestämmelsernas rättsligt bindande natur, såväl internt som externt,

d) tillämpningen av allmänna principer för dataskydd, särskilt avgränsning av syften, uppgiftsminimering, begränsade lagringsperioder, datakvalitet, inbyggt dataskydd och dataskydd som standard, rättslig grund för behandling, behandling av särskilda kategorier av personuppgifter, åtgärder för att säkerställa datasäkerhet och villkoren när det gäller vidare överföring av uppgifter till organ som inte är bundna av bindande företagsbestämmelser,

e) de registrerades rättigheter avseende behandling och medlen för att utöva dessa rättigheter, inklusive rätten att inte bli föremål för beslut grundade enbart på automatisk behandling, inklusive profilering, enligt artikel 22, rätten att inge klagomål till den behöriga tillsynsmyndigheten och till behöriga domstolar i medlemsstaterna enligt artikel 79, rätten till prövning samt i förekommande fall rätten till kompensation för överträdelse av de bindande företagsbestämmelserna,

f) att den personuppgiftsansvarige eller personuppgiftsbiträdet som är etablerad inom en medlemsstats territorium tar på sig ansvaret om en berörd enhet som inte är etablerad inom unionen bryter mot de bindande företagsbestämmelserna; den personuppgiftsansvarige eller personuppgiftsbiträdet får helt eller delvis undantas från denna skyldighet endast på villkor att det kan visas att den berörda enheten i företagsgruppen inte kan hållas ansvarig för den skada som har uppkommit,

g) hur de registrerade ska informeras om innehållet i de bindande företagsbestämmelserna, särskilt de bestämmelser som avses i leden d, e och f i denna punkt utöver den information som avses i artiklarna 13 och 14,

h) uppgifterna för varje dataskyddsombud som utsetts i enlighet med artikel 37, eller varje annan person eller enhet med ansvar för kontrollen av att de bindande företagsbestämmelserna följs inom den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet, samt i fråga om utbildning och hantering av klagomål,

i) förfaranden för klagomål,

j) rutinerna inom den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet för att kontrollera att de bindande företagsreglerna följs; sådana rutiner ska inbegripa dataskyddstillsyn och metoder för att säkerställa korrigerande åtgärder för att skydda de registrerades rättigheter; resultaten av sådana kontroller bör meddelas den person eller enhet som avses i led h och styrelsen i det kontrollerande företaget i koncernen eller gruppen av företag som deltar i gemensam ekonomisk verksamhet, och bör på begäran vara tillgänglig för den behöriga tillsynsmyndigheten,

k) rutinerna för att rapportera och dokumentera ändringar i bestämmelserna, samt rutinerna för att rapportera dessa ändringar till tillsynsmyndigheten,

l) rutinerna för att samarbeta med tillsynsmyndigheten i syfte att se till att alla medlemmar i den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet följer reglerna, särskilt genom att meddela tillsynsmyndigheten resultaten av kontroller av de åtgärder som avses i led j,

m) rutinerna för att till den behöriga tillsynsmyndigheten rapportera alla rättsliga krav som en medlem i koncernen eller gruppen av företag som deltar i gemensam ekonomisk verksamhet är underkastad i ett 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 omöverföringen 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 anförtrotts utnämningen.

2. Varje ledamot ska ha de kvalifikationer, den erfarenhet och den kompetens, särskilt på området skydd av personuppgifter, som krävs för att ledamoten ska kunna utföra sitt uppdrag och utöva sina befogenheter.

3. En ledamots uppdrag ska upphöra då mandattiden löper ut eller om ledamoten avgår eller avsätts från sin tjänst i enlighet med den berörda medlemsstatens nationella rätt.

4. En ledamot får avsättas endast på grund av grov försummelse eller när ledamoten inte längre uppfyller de villkor som krävs för att utföra uppdraget.

Artikel 54

Regler för inrättandet av en tillsynsmyndighet

1. Varje medlemsstat ska fastställa följande i lag:

a) Varje tillsynsmyndighets inrättande.

b) De kvalifikationer och de villkor för lämplighet som krävs för att någon ska kunna 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 överträdelser 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 personuppgiftsbiträdets huvudsakliga verksamhetsställe eller enda verksamhetsställe vara behörig att agera som ansvarig tillsynsmyndighet för den personuppgiftsansvariges eller personuppgiftsbiträdets 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 personuppgiftsbiträdet 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 personuppgiftsbiträdets enda motpart när det gäller den registreringsansvariges eller den personuppgiftsbiträdets gränsöverskridande behandling.

Artikel 57

Uppgifter

1. Utan att det påverkar de andra uppgifter som föreskrivs i denna förordning ska varje tillsynsmyndighet på sitt territorium ansvara för följande:

a) Övervaka och verkställa tillämpningen av denna förordning.

b) Öka allmänhetens medvetenhet om och förståelse för risker, regler, skyddsåtgärder och rättigheter i fråga om behandling. Särskild uppmärksamhet ska ägnas åt insatser som riktar sig till barn.

c) I enlighet med medlemsstatens nationella rätt ge rådgivning åt det nationella parlamentet, regeringen och andra institutioner och organ om lagstiftningsåtgärder och administrativa åtgärder rörande skyddet av fysiska personers rättigheter och friheter när det gäller behandling.

d) Öka personuppgiftsansvarigas och personuppgiftsbiträdens 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. Utövandet av de befogenheter som tillsynsmyndigheten tilldelas enligt denna artikel ska omfattas av lämpliga skyddsåtgärder, inbegripet effektiva rättsmedel och rättssäkerhet, som fastställs i unionsrätten och i medlemsstaternas nationella rätt i enlighet med stadgan.

5. Varje medlemsstat ska i lagstiftning fastställa att dess tillsynsmyndighet ska ha befogenhet att upplysa de rättsliga myndigheterna om överträdelser av denna förordning och vid behov att inleda eller på övrigt vis delta i rättsliga förfaranden, för att verkställa bestämmelserna i denna förordning.

6. Varje medlemsstat får i lagstiftning föreskriva att dess tillsynsmyndighet ska ha ytterligare befogenheter utöver dem som avses i punkterna 1, 2 och 3. Utövandet av dessa befogenheter ska inte påverka den effektiva tillämpningen av kapitel VII.

Artikel 59

Verksamhetsrapporter

Varje tillsynsmyndighet ska upprätta en årlig rapport om sin verksamhet, vilken kan omfatta en förteckning över typer av anmälda överträdelser 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 personuppgiftsbiträdets 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 personuppgiftsbiträdets 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 utbytts 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 skyndsam handling för att skydda registrerades rättigheter och friheter, får vilken tillsynsmyndighet som helst begära ett brådskande yttrande eller, i tillämpliga fall, ett brådskande bindande beslut från styrelsen, varvid den ska motivera varför den begär ett sådant yttrande eller beslut och varför åtgärden måste vidtas skyndsamt.

4. Genom undantag från artiklarna 64.3 och 65.2 ska ett brådskande yttrande eller ett brådskande beslut enligt punkterna 2 och 3 i den här artikeln antas inom två veckor med enkel majoritet av styrelsens ledamöter.

Artikel 67

Utbyte av information

Kommissionen får anta genomförandeakter med allmän räckvidd i syfte att närmare ange tillvägagångssätten för elektroniskt utbyte av information mellan tillsynsmyndigheter samt mellan tillsynsmyndigheter och styrelsen, särskilt det standardiserade format som avses i artikel 64.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

Avsnitt 3

Europeiska dataskyddsstyrelsen

Artikel 68

Europeiska dataskyddsstyrelsen

1. Europeiska dataskyddsstyrelsen (nedan kallad *styrelsen*) inrättas härmed som ett unionsorgan och ska ha ställning som juridisk person.

2. Styrelsen ska företrädas av sin ordförande.

3. Styrelsen ska bestå av chefen för en tillsynsmyndighet per medlemsstat och av Europeiska datatillsynsmannen eller deras respektive företrädare.

4. Om en medlemsstat har mer än en tillsynsmyndighet som ansvarar för att övervaka tillämpningen av bestämmelserna i denna förordning ska en gemensam företrädare utses i enlighet med den medlemsstatens nationella rätt.

5. Kommissionen ska ha rätt att delta i styrelsens verksamhet och möten utan rösträtt. Kommissionen ska utse en egen företrädare. Styrelsens ordförande ska underrätta kommissionen om styrelsens verksamhet.

6. I de fall som avses i artikel 65 ska Europeiska datatillsynsmannen endast ha rösträtt i fråga om beslut som rör principer och regler som är tillämpliga på unionens institutioner, organ och byråer, och som i allt väsentligt motsvarar dem i denna förordning.

Artikel 69

Oberoende

1. Styrelsen ska vara oberoende när den fullgör sina uppgifter eller utövar sina befogenheter i enlighet med artiklarna 70 och 71.

2. Utan att detta påverkar kommissionens rätt att lämna en begäran enligt artikel 70.1 b och 70.2 ska styrelsen när den fullgör sina uppgifter eller utövar sina befogenheter varken begära eller ta emot instruktioner av någon.

Artikel 70

Styrelsens uppgifter

1. Styrelsen ska se till att denna förordning tillämpas enhetligt. För detta ändamål ska styrelsen, på eget initiativ eller i förekommande fall på begäran av kommissionen, i synnerhet

a) övervaka och säkerställa korrekt tillämpning av denna förordning i de fall som avses i artiklarna 64 och 65 utan att det påverkar de nationella tillsynsmyndigheternas uppgifter,

b) ge kommissionen råd i alla frågor som gäller skydd av personuppgifter inom unionen, inklusive om eventuella förslag till ändring av denna förordning,

c) ge kommissionen råd om format och förfaranden för informationsutbyte mellan personuppgiftsansvariga, personuppgiftsbiträden och tillsynsmyndigheter för bindande företagsbestämmelser,

d) utfärda riktlinjer, rekommendationer och bästa praxis beträffande förfaranden för att radera länkar, kopior eller reproduktioner av personuppgifter från allmänt tillgängliga kommunikationstjänster enligt artikel 17.2,

e) på eget initiativ eller på begäran av en av sina ledamöter eller av kommissionen behandla frågor om tillämpningen av denna förordning och utfärda riktlinjer, rekommendationer och bästa praxis i syfte att främja en enhetlig tillämpning av denna förordning,

f) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att närmare ange kriterierna och villkoren för profileringsbaserade beslut enligt artikel 22.2,

g) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att konstatera sådana personuppgiftsincidenter och fastställa sådant onödigt dröjsmål som avses i artikel 33.1 och 33.2 och för de särskilda omständigheter under vilka en personuppgiftsansvarig eller ett personuppgiftsbiträde är skyldig att anmäla personuppgiftsincidenten,

h) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt angående de omständigheter under vilka en personuppgiftsincident sannolikt kommer att leda till hög risk för rättigheterna och friheterna för de fysiska personer som avses i artikel 34.1,

i) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att närmare ange kriterierna och kraven för överföringar av personuppgifter på grundval av bindande företagsbestämmelser som personuppgiftsansvariga eller personuppgiftsbiträden följer samt ytterligare nödvändiga krav för att säkerställa skyddet för personuppgifter för berörda registrerade enligt artikel 47,

j) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att närmare ange kriterierna och villkoren för överföring av personuppgifter på grundval av artikel 49.1,

k) utforma riktlinjer för tillsynsmyndigheterna i fråga om tillämpningen av de åtgärder som avses i artikel 58.1, 58.2 och 58.3 och fastställandet av administrativa sanktionsavgifter i enlighet med artikel 83,

l) se över den praktiska tillämpningen av de riktlinjer och rekommendationer samt den bästa praxis som avses i leden e och f,

m) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att fastställa gemensamma förfaranden för fysiska personers rapportering av överträdelser av denna förordning enligt artikel 54.2,

n) främja utarbetandet av uppförandekoder och införandet av certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd i enlighet med artiklarna 40 och 42,

o) ackreditera certifieringsorgan och utföra sin periodiska översyn i enlighet med artikel 43 och föra ett offentligt register över ackrediterade organ i enlighet med artikel 43.6 och över de ackrediterade personuppgiftsansvariga eller personuppgiftsbiträdena som är etablerade i tredjeländer i enlighet med artikel 42.7,

p) närmare ange de krav som avses i artikel 43.3 i syfte att ackreditera certifieringsorgan enligt artikel 42,

q) avge ett yttrande till kommissionen om de certifieringskrav som avses i artikel 43.8,

r) avge ett yttrande till kommissionen om de symboler som avses i artikel 12.7,

s) avge ett yttrande till kommissionen för bedömningen av adekvat skyddsnivå i ett tredjeland eller en internationell organisation, inklusive för bedömningen av huruvida ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom det tredjelandet, eller en internationell organisation inte längre säkerställer en adekvat skyddsnivå; i detta syfte ska kommissionen lämna all nödvändig dokumentation till styrelsen, inklusive korrespondens med regeringen i tredjelandet, med avseende på tredjelandet, territoriet eller den specificerade sektorn, eller till databehandlingssektorn i tredjelandet eller den internationella organisationen,

t) avge yttranden om utkast till beslut som läggs fram av tillsynsmyndigheter inom den mekanism för enhetlighet som avses i artikel 64.1, i ärenden som ingivits i enlighet med artikel 64.2 och anta bindande beslut i enlighet med artikel 65, inbegripet de fall som avses i artikel 66,

u) främja samarbete och effektivt bilateralt och multilateralt utbyte av bästa praxis och information mellan tillsynsmyndigheterna,

v) främja gemensamma utbildningsprogram och underlätta personalutbyte mellan tillsynsmyndigheterna och där så är lämpligt även med tillsynsmyndigheter i tredjeländer eller internationella organisationer,

w) främja utbyte av kunskap och dokumentation om lagstiftning om och praxis för dataskydd med tillsynsmyndigheter för dataskydd i hela världen.

x) avge yttranden över de uppförandekoder som utarbetas på unionsnivå i enlighet med artikel 40.9, och

y) föra ett offentligt elektroniskt register över tillsynsmyndigheters beslut och domstolars avgöranden i frågor som hanteras inom mekanismen för enhetlighet.

2. När kommissionen begär rådgivning från styrelsen får den ange en tidsfrist med hänsyn till hur brådskande ärendet är.

3. Styrelsen ska vidarebefordra sina yttranden, riktlinjer, rekommendationer och bästa praxis till kommissionen och till den kommitté som avses i artikel 93, samt offentliggöra dem.

4. När så är lämpligt ska styrelsen samråda med berörda parter och ge dem möjlighet att yttra sig inom rimlig tid. styrelsen ska, utan att det påverkar tillämpningen av artikel 76, offentliggöra resultatet av samrådsförfarandet.

Artikel 71

Rapporter

1. Styrelsen ska sammanställa en årsrapport om skydd av fysiska personer vid behandling inom unionen och, i förekommande fall, i tredjeländer och internationella organisationer. Rapporten ska offentliggöras och översändas till Europaparlamentet, rådet och kommissionen.

2. Årsrapporten ska också innehålla en översikt över den praktiska tillämpningen av de riktlinjer och rekommendationer och den bästa praxis som avses i artikel 70.1 l liksom de bindande beslut som avses i artikel 65.

Artikel 72

Förfarande

1. Styrelsen ska fatta beslut med enkel majoritet av dess ledamöter, om inte annat anges i denna förordning.

2. Styrelsen ska själv anta sin arbetsordning med två tredjedels majoritet av sina ledamöter och fastställa sina arbetsformer.

Artikel 73

Ordförande

1. Styrelsen ska med enkel majoritet välja en ordförande och två vice ordförande bland sina ledamöter.

2. Ordförandens och de vice ordförandenas mandattid ska vara fem år och kunna förnyas en gång.

Artikel 74

Ordförandens uppgifter

1. Ordföranden ska ha i uppgift att

a) sammankalla till styrelsens möten och planera dagordningen,

b) meddela beslut som antas av styrelsen i enlighet med artikel 65 till den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna,

c) se till att styrelsens uppgifter fullgörs i tid, särskilt i fråga om den mekanism för enhetlighet som avses i artikel 63.

2. Fördelningen av uppgifter mellan ordföranden och de vice ordförandena ska fastställas i styrelsens arbetsordning.

Artikel 75

Sekretariatet

1. Styrelsen ska förfoga över ett sekretariat som ska tillhandahållas av Europeiska datatillsynsmannen.

2. Sekretariatet ska utföra sina uppgifter enbart under ledning av ordföranden för styrelsen.

3. Den personal vid Europeiska datatillsynsmannen som utför de uppgifter som styrelsen tilldelas genom denna förordning ska följa separata rapporteringsvägar från den personal som utför de uppgifter som Europeiska datatillsynsmannen tilldelas.

4. När så är lämpligt ska styrelsen och Europeiska datatillsynsmannen fastställa och offentliggöra ett samförståndsavtal för genomförande av denna artikel, som fastställer villkoren för deras samarbete, och som ska tillämpas på den personal vid Europeiska datatillsynsmannen som utför de uppgifter som styrelsen tilldelas genom denna förordning.

5. Sekretariatet ska förse styrelsen med analysstöd samt administrativt och logistiskt stöd.

6. Sekretariatet ska särskilt ansvara för

a) styrelsens löpande arbete,

b) kommunikationen mellan styrelsens ledamöter, dess ordförande och kommissionen,

c) kommunikationen med andra institutioner och med allmänheten,

d) användningen av elektroniska medel för intern och extern kommunikation,

e) översättning av relevant information,

f) förberedelser och uppföljning av styrelsens möten,

g) förberedelse, sammanställning och offentliggörande av yttranden, beslut om lösning av tvister mellan tillsynsmyndigheter och andra texter som antas av styrelsen.

Artikel 76

Konfidentialitet

1. Styrelsens överläggningar ska vara konfidentiella i de fall som styrelsen bedömer detta vara nödvändigt, i enlighet med vad som anges i dess arbetsordning.

2. Tillgången till handlingar som skickas till styrelsens ledamöter, till experter eller till företrädare för tredje part ska regleras av Europaparlamentets och rådets förordning (EG) nr 1049/2001 ([1]).

KAPITEL VIII

Rättsmedel, ansvar och sanktioner

Artikel 77

Rätt att lämna in klagomål till en tillsynsmyndighet

1. Utan att det påverkar något annat administrativt prövningsförfarande eller rättsmedel, ska varje registrerad som anser att behandlingen av personuppgifter som avser henne eller honom strider mot denna förordning ha rätt att lämna in ett klagomål till en tillsynsmyndighet, särskilt i den medlemsstat där han eller hon har sin hemvist eller sin arbetsplats eller där det påstådda intrånget begicks.

2. Den tillsynsmyndighet till vilken klagomålet har ingetts ska underrätta den enskilde om hur arbetet med klagomålet fortskrider och vad resultatet blir, inbegripet möjligheten till rättslig prövning enligt artikel 78.

Artikel 78

Rätt till ett effektivt rättsmedel mot tillsynsmyndighetens beslut

1. Utan att det påverkar något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol ska varje fysisk eller juridisk person ha rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut rörande dem som meddelats av en tillsynsmyndighet.

2. Utan att det påverkar något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol, ska varje registrerad person ha rätt till ett effektivt rättsmedel om den tillsynsmyndighet som är behörig i enlighet med artiklarna 55 och 56 underlåter att behandla ett klagomål eller att informera den registrerade inom tre månader om hur det fortskrider med det klagomål som ingetts med stöd av artikel 77 eller vilket beslut som har fattats med anledning av det.

3. Talan mot en tillsynsmyndighet ska väckas vid domstolarna i den medlemsstat där tillsynsmyndigheten har sitt säte.

4. Om talan väcks mot ett beslut som fattats av en tillsynsmyndighet och som föregicks av ett yttrande från eller beslut av styrelsen inom ramen för mekanismen för enhetlighet ska tillsynsmyndigheten vidarebefordra detta yttrande eller beslut till domstolen.

Artikel 79

Rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde

1. Utan att det påverkar tillgängliga administrativa prövningsförfaranden eller prövningsförfaranden utanför domstol, inbegripet rätten att lämna in ett klagomål till en tillsynsmyndighet i enlighet med artikel 77, ska varje registrerad som anser att hans eller hennes rättigheter enligt denna förordning har åsidosatts som en följd av att hans eller hennes personuppgifter har behandlats på ett sätt som inte är förenligt med denna förordning ha rätt till ett effektivt rättsmedel.

2. Talan mot en personuppgiftsansvarig eller ett personuppgiftsbiträde ska väckas vid domstolarna i den medlemsstat där den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad. Alternativt får sådan talan väckas vid domstolarna i den medlemsstat där den registrerade har sin hemvist, såvida inte den personuppgiftsansvarige eller personuppgiftsbiträdet är en myndighet i en medlemsstat som agerar inom ramen för sin myndighetsutövning.

([1]) Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar (EGT L 145, 31.5.2001, s. 43).

Artikel 80

Företrädande av registrerade

1. Den registrerade ska ha rätt att ge ett organ, en organisation eller sammanslutning utan vinstsyfte, som har inrättats på lämpligt sätt i enlighet med lagen i en medlemsstat, vars stadgeenliga mål är av allmänt intresse och som är verksam inom området skydd av registrerades rättigheter och friheter när det gäller skyddet av deras personuppgifter, i uppdrag att lämna in ett klagomål för hans eller hennes räkning, att utöva de rättigheter som avses i artiklarna 77, 78 och 79 för hans eller hennes räkning samt att för hans eller hennes räkning utöva den rätt till ersättning som avses i artikel 82 om så föreskrivs i medlemsstatens nationella rätt.

2. Medlemsstaterna får föreskriva att ett organ, en organisation eller en sammanslutning enligt punkt 1 i den här artikeln, oberoende av en registrerads mandat, har rätt att i den medlemsstaten inge klagomål till den tillsynsmyndighet som är behörig enligt artikel 77 och utöva de rättigheter som avses i artiklarna 78 och 79 om organet, organisationen eller sammanslutningen anser att den registrerades rättigheter enligt den här förordningen har kränkts som en följd av behandlingen.

Artikel 81

Vilandeförklaring av förfaranden

1. Om en behörig domstol i en medlemsstat har information om att förfaranden som rör samma sakfråga vad gäller behandling av samma personuppgiftsansvarige eller personuppgiftsbiträde pågår i en domstol i en annan medlemsstat ska den kontakta denna domstol i den andra medlemsstaten för att bekräfta förekomsten av sådana förfaranden.

2. Om förfaranden som rör samma sakfråga vad gäller behandling av samma personuppgiftsansvarige eller personuppgiftsbiträde pågår i en domstol i en annan medlemstat 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 uppgiftsbehandlingens karaktär, omfattning eller syfte samt antalet berörda registrerade och den skada som de har lidit.

b) Om överträdelsen skett med uppsåt eller genom oaktsamhet.

c) De åtgärder som den personuppgiftsansvarige eller personuppgiftsbiträdet har vidtagit för att lindra den skada som de registrerade har lidit.

d) Graden av ansvar hos den personuppgiftsansvarige eller personuppgiftsbiträdet med beaktande av de tekniska och organisatoriska åtgärder som genomförts av dem i enlighet med artiklarna 25 och 32.

e) Eventuella relevanta tidigare överträdelser som den personuppgiftsansvarige eller personuppgiftsbiträdet gjort sig skyldig till.

f) Graden av samarbete med tillsynsmyndigheten för att komma till rätta med överträdelsen och minska dess potentiella negativa effekter.

g) De kategorier av personuppgifter som påverkas av överträdelsen.

h) Det sätt på vilket överträdelsen kom till tillsynsmyndighetens kännedom, särskilt huruvida och i vilken omfattning den personuppgiftsansvarige eller personuppgiftsbiträdet anmälde överträdelsen.

i) När åtgärder enligt artikel 58.2 tidigare har förordnats mot den berörda personuppgiftsansvarige eller personuppgiftsbiträdet vad gäller samma sakfråga, efterlevnad av dessa åtgärder.

j) Tillämpandet av godkända uppförandekoder i enlighet med artikel 40 eller godkända certifieringsmekanismer i enlighet med artikel 42.

k) Eventuell annan försvårande eller förmildrande faktor som är tillämplig på omständigheterna i fallet, såsom ekonomisk vinst som görs eller förlust som undviks, direkt eller indirekt, genom överträdelsen.

3. Om en personuppgiftsansvarig eller ett personuppgiftsbiträde, med avseende på en och samma eller sammankopplade uppgiftsbehandlingar, uppsåtligen eller av oaktsamhet överträder flera av bestämmelserna i denna förordning får den administrativa sanktionsavgiftens totala belopp inte överstiga det belopp som fastställs för den allvarligaste överträdelsen.

4. Vid överträdelser av följande bestämmelser ska det i enlighet med punkt 2 påföras administrativa sanktionsavgifter på upp till 10 000 000 EUR eller, om det gäller ett företag, på upp till 2 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

a) Personuppgiftsansvarigas och personuppgiftsbiträdens 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 underlåtelse att ge tillgång till uppgifter i strid med artikel 58.1.

6. Vid underlåtenhet att rätta sig efter ett föreläggande från tillsynsmyndigheten i enlighet med artikel 58.2 ska det i enlighet med punkt 2 i den här artikeln påföras administrativa sanktionsavgifter på upp till 20 000 000 EUR eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

7. Utan att det påverkar tillsynsmyndigheternas korrigerande befogenheter enligt artikel 58.2 får varje medlemsstat fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter och organ som är inrättade i medlemsstaten.

8. Tillsynsmyndighetens utövande av sina befogenheter enligt denna artikel ska omfattas av lämpliga rättssäkerhetsgarantier i enlighet med unionsrätten och medlemsstaternas nationella rätt, inbegripet effektiva rättsmedel och rättssäkerhet.

9. Om det i medlemsstatens rättssystem inte finns några föreskrifter om administrativa sanktionsavgifter får den här artikeln tillämpas så att förfarandet inleds av den behöriga tillsynsmyndigheten och sanktionsavgifterna sedan utdöms av behörig nationell domstol, varvid det säkerställs att rättsmedlen är effektiva och har motsvarande verkan som de administrativa sanktionsavgifter som påförs av tillsynsmyndigheter. De sanktionsavgifter som påförs ska i alla händelser vara effektiva, proportionella och avskräckande. Dessa medlemsstater ska till kommissionen anmäla de bestämmelser i deras lagstiftning som de antar i enlighet med denna punkt senast den 25 maj 2018, samt utan dröjsmål anmäla eventuell senare ändringslagstiftning eller ändringar som berör dem.

Artikel 84

Sanktioner

1. Medlemsstaterna ska fastställa regler om andra sanktioner för överträdelser av denna förordning, särskilt för överträdelser som inte är föremål för administrativa sanktionsavgifter enligt artikel 83, och vidta alla nödvändiga åtgärder för att säkerställa att de genomförs. Dessa sanktioner ska vara effektiva, proportionella och avskräckande.

2. Varje medlemsstat ska till kommissionen anmäla de bestämmelser i sin lagstiftning som den antar i enlighet med punkt 1 senast den 25 maj 2018, samt utan dröjsmål anmäla eventuella senare ändringar som berör dem.

KAPITEL IX

Bestämmelser om särskilda behandlingssituationer

Artikel 85

Behandling och yttrande- och informationsfriheten

1. Medlemsstaterna ska i lag förena rätten till integritet i enlighet med denna förordning med yttrande- och informationsfriheten, inbegripet behandling som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

2. Medlemsstaterna ska, för behandling som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande, fastställa undantag eller avvikelser från kapitel II (principer), kapitel III (den registrerades rättigheter), kapitel IV (personuppgiftsansvarig och personuppgiftsbiträde), kapitel V (överföring av personuppgifter till tredjeländer eller internationella organisationer), kapitel VI (oberoende tillsynsmyndigheter), kapitel VII (samarbete och enhetlighet) och kapitel IX (särskilda situationer vid behandling av personuppgifter) om dessa är nödvändiga för att förena rätten till integritet med yttrande- och informationsfriheten.

3. Varje medlemsstat ska till kommissionen anmäla de bestämmelser i sin lagstiftning som den antagit i enlighet med punkt 2, samt utan dröjsmål anmäla eventuell senare ändringslagstiftning eller ändringar som berör dem.

Artikel 86

Behandling och allmänhetens tillgång till allmänna handlingar

Personuppgifter i allmänna handlingar som förvaras av en myndighet eller ett offentligt organ eller ett privat organ för utförande av en uppgift av allmänt intresse får lämnas ut av myndigheten eller organet i enlighet med den unionsrätt eller den medlemsstats nationella rätt som myndigheten eller det offentliga organet omfattas av, för att jämka samman allmänhetens rätt att få tillgång till allmänna handlingar med rätten till skydd av personuppgifter i enlighet med denna förordning.

Artikel 87

Behandling av nationella identifikationsnummer

Medlemsstaterna får närmare bestämma på vilka särskilda villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas. Ett nationellt identifikationsnummer eller ett annat vedertaget sätt för identifiering ska i sådana fall endast användas med iakttagande av lämpliga skyddsåtgärder för de registrerades rättigheter och friheter enligt denna förordning.

Artikel 88

Behandling i anställningsförhållanden

1. Medlemsstaterna får i lag eller i kollektivavtal fastställa mer specifika regler för att säkerställa skyddet av rättigheter och friheter vid behandling av anställdas personuppgifter i anställningsförhållanden, särskilt när det gäller rekrytering, genomförande av anställningsavtalet inklusive befrielse från i lag eller kollektivavtal stadgade skyldigheter, ledning, planering och organisering av arbetet, jämställdhet och mångfald i arbetslivet, hälsa och säkerhet på arbetsplatsen samt skydd av arbetsgivarens eller kundens egendom men också när det gäller att såväl kollektivt som individuellt utöva och komma i åtnjutande av rättigheter och förmåner som är knutna till anställningen samt att avsluta anställningsförhållandet.

2. Dessa regler ska innehålla lämpliga och specifika åtgärder för att skydda den registrerades mänskliga värdighet, berättigade intressen och grundläggande rättigheter, varvid hänsyn särskilt ska tas till insyn i behandlingen, överföring av personuppgifter inom en koncern eller en grupp av företag som deltar i gemensam ekonomisk verksamhet samt övervakningssystem på arbetsplatsen.

3. Varje medlemsstat ska till kommissionen anmäla de bestämmelser i sin lagstiftning som den antar i enlighet med punkt 1 senast den 25 maj 2018, samt utan dröjsmål anmäla eventuella senare ändringar som berör dem.

Artikel 89

Skyddsåtgärder och undantag för behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål

1. Behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål ska omfattas av lämpliga skyddsåtgärder i enlighet med denna förordning för den registrerades rättigheter och friheter. Skyddsåtgärderna ska säkerställa att tekniska och organisatoriska åtgärder har införts för att se till att särskilt

principen om uppgiftsminimering iakttas. Dessa åtgärder får inbegripa pseudonymisering, under förutsättning att dessa ändamål kan uppfyllas på det sättet. När dessa ändamål kan uppfyllas genom vidare behandling av uppgifter som inte medger eller inte längre medger identifiering av de registrerade ska dessa ändamål uppfyllas på det sättet.

2. Om personuppgifter behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål får det i unionsrätten eller i medlemsstaternas nationella rätt föreskrivas undantag från de rättigheter som avses i artiklarna 15, 16, 18 och 21 med förbehåll för de villkor och skyddsåtgärder som avses i punkt 1 i den här artikeln i den utsträckning som sådana rättigheter sannolikt kommer att göra det omöjligt eller mycket svårare att uppfylla de särskilda ändamålen, och sådana undantag krävs för att uppnå dessa ändamål.

3. Om personuppgifter behandlas för arkivändamål av allmänt intresse får det i unionsrätten eller i medlemsstaternas nationella rätt föreskrivas om undantag från de rättigheter som avses i artiklarna 15, 16, 18, 19, 20 och 21 med förbehåll för de villkor och skyddsåtgärder som avses i punkt 1 i den här artikeln i den utsträckning som sådana rättigheter sannolikt kommer att göra det omöjligt eller mycket svårare att uppfylla de särskilda ändamålen, och sådana undantag krävs för att uppnå dessa ändamål.

4. Om behandling enligt punkterna 2 och 3 samtidigt har andra ändamål, ska undantagen endast tillämpas på behandling för de ändamål som avses i dessa punkter.

Artikel 90

Tystnadsplikt

1. Medlemsstaterna får anta särskilda bestämmelser för att fastställa tillsynsmyndigheternas befogenheter enligt artikel 58.1 e och f gentemot personuppgiftsansvariga eller personuppgiftsbiträden som enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställts av behöriga nationella organ omfattas av tystnadsplikt eller andra motsvarande former av förbud mot att lämna ut uppgifter, om det är nödvändigt och står i proportion till vad som behövs för att förena rätten till skydd för personuppgifter och tystnadsplikten. Dessa bestämmelser ska endast tillämpas med avseende på personuppgifter som den personuppgiftsansvarige eller personuppgiftsbiträdet har erhållit i samband med en verksamhet som omfattas av denna tystnadsplikt.

2. Varje medlemsstat ska till kommissionen anmäla de bestämmelser den har antagit i enlighet med punkt 1 senast den 25 maj 2018, samt utan dröjsmål anmäla eventuella ändringar som berör dem.

Artikel 91

Befintliga bestämmelser om dataskydd inom kyrkor och religiösa samfund

1. Om kyrkor och religiösa samfund eller gemenskaper i en medlemsstat vid tidpunkten för ikraftträdandet av denna förordning tillämpar övergripande bestämmelser om skyddet av fysiska personer i samband med behandling, får sådana befintliga bestämmelser fortsätta att tillämpas under förutsättning att de görs förenliga med denna förordning.

2. Kyrkor och religiösa samfund som tillämpar övergripande bestämmelser i enlighet med punkt 1 i denna artikel ska vara föremål för kontroll av en oberoende tillsynsmyndighet som kan vara specifik, förutsatt att den uppfyller de villkor som fastställs i kapitel VI i denna förordning.

KAPITEL X

Delegerade akter och genomförandeakter

Artikel 92

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artikel 12.8 och artikel 43.8 ska ges till kommissionen tills vidare från och med den 24 maj 2016.

3. Den delegering av befogenhet som avses i artikel 12.8 och artikel 43.8 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

5. En delegerad akt som antas enligt artikel 12.8 och artikel 43.8 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period av tre månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med tre månader på Europaparlamentets eller rådets initiativ.

Artikel 93

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

3. När det hänvisas till denna punkt ska artikel 8 i förordning (EU) nr 182/2011, jämförd med artikel 5 i samma förordning, tillämpas.

KAPITEL XI

Slutbestämmelser

Artikel 94

Upphävande av direktiv 95/46/EG

1. Direktiv 95/46/EG ska upphöra att gälla med verkan från och med den 25 maj 2018.

2. Hänvisningar till det upphävda direktivet ska anses som hänvisningar till denna förordning. Hänvisningar till arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter, som inrättades genom artikel 29 i direktiv 95/46/EG, ska anses som hänvisningar till Europeiska dataskyddsstyrelsen, som inrättas genom denna förordning.

Artikel 95

Förhållande till direktiv 2002/58/EG

Denna förordning ska inte innebära några ytterligare förpliktelser för fysiska eller juridiska personer som behandlar personuppgifter inom ramen för tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät i unionen, när det gäller områden inom vilka de redan omfattas av särskilda skyldigheter för samma ändamål i enlighet med direktiv 2002/58/EG.

Artikel 96

Förhållande till tidigare ingångna avtal

De internationella avtal som rör överföring av personuppgifter till tredjeländer eller internationella organisationer som ingicks av medlemsstaterna före den 24 maj 2016 och som är förenliga med unionsrätten i dess lydelse innan detta datum, ska fortsätta att gälla tills de ändras, ersätts eller återkallas.

Artikel 97

Kommissionsrapporter

1. Senast den 25 maj 2020 och därefter vart fjärde år ska kommissionen överlämna en rapport om tillämpningen och översynen av denna förordning till Europaparlamentet och rådet.

2. Inom ramen för de utvärderingar och översyner som avses i punkt 1 ska kommissionen särskilt undersöka hur följande bestämmelser tillämpas och fungerar:

a) Kapitel V om överföring av personuppgifter till tredjeländer och internationella organisationer, särskilt när det gäller beslut som antagits enligt artikel 45.3 i den här förordningen och beslut som antagits på grundval av artikel 25.6 i direktiv 95/46/EG.

b) Kapitel VII om samarbete och enhetlighet.

3. Med avseende på tillämpningen av punkt 1 får kommissionen begära information från medlemsstaterna och tillsynsmyndigheterna.

4. Kommissionen ska när den utför de utvärderingar och översyner som avses i punkterna 1 och 2 ta hänsyn till ståndpunkter och slutsatser från Europaparlamentet, rådet och andra relevanta organ och källor.

5. Kommissionen ska om nödvändigt överlämna lämpliga förslag om ändring av denna förordning, med särskild hänsyn till informationsteknikens utveckling och mot bakgrund av tendenserna inom 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.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 27 april 2016.

På Europaparlamentets vägnar	*På rådets vägnar*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT
Ordförande	*Ordförande*