Lagrådsremiss

Ny kamerabevakningslag

Regeringen överlämnar denna remiss till Lagrådet.

Stockholm den 8 mars 2018

Peter Hultqvist

David Törngren
(Justitiedepartementet)

Lagrådsremissens huvudsakliga innehåll

Regeringen föreslår att kameraövervakningslagen upphävs och att en ny lag om kamerabevakning införs. Genom den nya lagen förbättras möjligheterna att använda kamerabevakning samtidigt som integritetsskyddet förstärks. Regleringen anpassas också till de nya EU-reglerna om dataskydd. Förslaget innebär bl.a. följande.

- Den nya lagen kommer bara att vara tillämplig när kameror används på ett sätt som innebär personbevakning.
- Kravet på tillstånd begränsas till myndigheter och vissa andra som utför uppgifter av allmänt intresse.
- Det blir lättare för Polismyndigheten och kommuner att få tillstånd till kamerabevakning på offentliga platser, i brottsbekämpande eller trygghetsskapande syften.
- Polismyndigheten och Säkerhetspolisen får utökade möjligheter att tillfälligt använda kamerabevakning utan tillstånd vid risk för allvarlig brottslighet.
- Möjligheterna att få tillstånd till kamerabevakning bl.a. på tåg och stationer samt inom hälso- och sjukvården förbättras.
- En upplysning införs om att det vid arbetsgivares kamerabevakning av arbetsplatser finns bestämmelser om förhandlingsskyldighet i lagen om medbestämmande i arbetslivet.
- En och samma myndighet ska pröva frågor om tillstånd och utöva tillsyn enligt lagen.

Vidare föreslås vissa ändringar i offentlighets- och sekretesslagen.
Lagändringarna föreslås träda i kraft den 1 augusti 2018.

Innehållsförteckning

1 Beslut

Regeringen har beslutat att inhämta Lagrådets yttrande över förslag till

1. kamerabevakningslag,
2. lag om ändring i offentlighets- och sekretesslagen (2009:400).

2 Lagtext

Regeringen har följande förslag till lagtext.

2.1 Förslag till kamerabevakningslag

Härigenom föreskrivs[1] följande.

Allmänna bestämmelser

1 § I denna lag finns bestämmelser om kamerabevakning som

– kompletterar Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), här benämnd EU:s dataskyddsförordning, och

– genomför 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, här benämnt EU:s dataskyddsdirektiv.

I lagen finns också bestämmelser om sådan kamerabevakning som inte omfattas av EU:s dataskyddsförordning eller EU:s dataskyddsdirektiv.

Lagens syfte

2 § Syftet med denna lag är att tillgodose behovet av kamerabevakning för berättigade ändamål och att skydda fysiska personer mot otillbörligt intrång i den personliga integriteten vid sådan bevakning.

Kamerabevakning

3 § Med kamerabevakning avses

1. att en tv-kamera, ett annat optisk-elektroniskt instrument eller en därmed jämförbar utrustning, utan att manövreras på platsen, används på ett sätt som innebär varaktig eller regelbundet upprepad personbevakning,

2. att en separat teknisk anordning för avlyssning eller upptagning av ljud används i samband med sådan användning av utrustning som avses i 1, eller

3. att en separat teknisk anordning används för att behandla bild- och ljudmaterial som tagits upp med sådan utrustning som avses i 1 eller 2.

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

Lagens tillämpningsområde

4 § Lagen gäller endast om

1. kamerabevakning enligt 3 § 1 eller 2 sker med utrustning som finns i Sverige och den som bedriver bevakningen är etablerad i Sverige eller i tredjeland, eller
2. kamerabevakning enligt 3 § 3 avser behandling av bild- och ljudmaterial som tagits upp vid bevakning som avses i 1 och behandlingen utförs av den som bedriver bevakningen eller för hans eller hennes räkning.

5 § Lagen gäller inte vid

1. kamerabevakning som en fysisk person utför som ett led i en verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll,
2. hemlig kameraövervakning enligt 27 kap. rättegångsbalken eller lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott,
3. kamerabevakning som sker i en verksamhet som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen, eller
4. kamerabevakning som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

Lagens förhållande till annan dataskyddsreglering

6 § Utöver vad som föreskrivs i denna lag gäller

1. EU:s dataskyddsförordning, lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning, föreskrifter som har meddelats i anslutning till den lagen och andra föreskrifter som kompletterar dataskyddsförordningen,
2. brottsdatalagen (2018:000), föreskrifter som har meddelats i anslutning till den lagen och andra föreskrifter som genomför EU:s dataskyddsdirektiv, och
3. föreskrifter om sådan behandling av personuppgifter som inte omfattas av dataskyddsförordningens eller brottsdatalagens tillämpningsområde.

Tillstånd till kamerabevakning

Krav på tillstånd

7 § Tillstånd till kamerabevakning av en plats dit allmänheten har tillträde krävs, om bevakningen ska bedrivas av

1. en myndighet, eller
2. någon annan än en myndighet vid utförande av en uppgift av allmänt intresse som följer av lag eller annan författning, kollektivavtal eller beslut som meddelats med stöd av lag eller annan författning.

Förutsättningar för tillstånd

8 § Tillstånd till kamerabevakning ska ges om intresset av sådan bevakning väger tyngre än den enskildes intresse av att inte bli bevakad.

Vid bedömningen av intresset av kamerabevakning ska det särskilt beaktas om bevakningen behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott på en brottsutsatt plats eller på en annan plats där det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet eller på egendom,
2. förebygga, förhindra eller upptäcka störningar av allmän ordning och säkerhet eller begränsa verkningarna av sådana störningar,
3. utöva kontrollverksamhet,
4. förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor, eller
5. tillgodose andra därmed jämförliga ändamål.

Vid bedömningen av den enskildes intresse av att inte bli bevakad ska det särskilt beaktas

1. hur bevakningen ska utföras,
2. om teknik som främjar skyddet av den enskildes personliga integritet ska användas, och
3. vilket område som ska bevakas.

Undantag från tillståndskravet

9 § Tillstånd till kamerabevakning krävs inte vid

1. bevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning,
2. bevakning som sker för att skydda en byggnad, en annan anläggning eller ett område som enligt 4 § 4, 5 § 1–5 eller 6 § första stycket skyddslagen (2010:305) har förklarats vara skyddsobjekt, om bevakningen endast omfattar skyddsobjektet eller ett område i dess omedelbara närhet,
3. bevakning som Försvarsmakten bedriver från ett fordon, fartyg eller luftfartyg som ett led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan bevakning,
4. bevakning som Trafikverket bedriver
   a) av vägtrafik,
   b) av sjötrafik vid en rörlig bro,
   c) vid en betalstation som avses i bilagorna till lagen (2004:629) om trängselskatt och som sker för att samla in uppgifter som behövs för att beslut om trängselskatt ska kunna fattas och för att kontrollera att sådan skatt betalas, eller
   d) vid en betalstation på allmän väg som används vid uttag av infrastrukturavgifter enligt lagen (2014:52) om infrastrukturavgifter på väg och som sker för att samla in uppgifter som behövs för att beslut om infrastrukturavgift ska kunna fattas och för att kontrollera att sådan avgift betalas,
5. bevakning i en vägtunnel med övervakningssystem som avses i lagen (2006:418) om säkerhet i vägtunnlar och som bedrivs av någon annan tunnelhållare än Trafikverket,
6. bevakning i en tunnelbanevagn eller av en tunnelbanestation, om bevakningen har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott eller förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor,

7. bevakning i en lokal där det bedrivs postverksamhet eller av området omedelbart utanför in- och utgångar till en sådan lokal, om bevakningen har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott,

8. bevakning i ett parkeringshus, om bevakningen har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott, och

9. bevakning som sker för säkerheten i trafiken eller arbetsmiljön från ett fordon, en maskin eller liknande för att förbättra sikten för föraren eller användaren.

Tillfälliga undantag från tillståndskravet

10 § Kamerabevakning får ske utan att en ansökan om tillstånd har gjorts

1. under högst tre månader, vid bevakning som bedrivs av Polismyndigheten eller Säkerhetspolisen, om det av särskild anledning finns risk för allvarlig brottslighet och syftet med bevakningen är att förebygga, förhindra eller upptäcka sådan brottslig verksamhet eller utreda eller lagföra sådana brott,

2. under högst en månad, vid bevakning som bedrivs av Polismyndigheten eller den som är räddningsledare enligt lagen (2013:778) om skydd mot olyckor, om bevakningen är av vikt för att avvärja en överhängande fara för olycka, begränsa verkningarna av en inträffad olycka eller minska risken för nya olyckor, eller

3. under högst en månad, vid bevakning som bedrivs av den som är räddningsledare enligt lagen om skydd mot olyckor, om bevakningen är av vikt för att efterforska en försvunnen person.

Om en ansökan om tillstånd görs inom den tid som anges i första stycket, får bevakningen bedrivas utan tillstånd till dess att ansökan har prövats.

Ansökan om tillstånd

11 § En ansökan om tillstånd till kamerabevakning ska göras skriftligen hos tillsynsmyndigheten.

Ansökan ska innehålla

1. uppgift om den som ska bedriva bevakningen och i förekommande fall den som ska ha hand om bevakningen för tillståndshavarens räkning,

2. uppgift om bevakningens ändamål,

3. en beskrivning av bevakningen, särskilt den utrustning som ska användas, var utrustningen ska placeras, det område eller typ av område som ska bevakas och de tider då bevakning ska ske,

4. en bedömning av behovet av bevakningen och bevakningens proportionalitet i förhållande till ändamålet,

5. en bedömning av riskerna för intrång i den personliga integriteten och en beskrivning av de åtgärder som planeras för att hantera riskerna, och

6. uppgift om de omständigheter i övrigt som är av betydelse för prövningen av ärendet.

Om sökanden inte är en myndighet, ska ansökan innehålla uppgift om den lag eller annan författning, kollektivavtal eller beslut som utgör den rättsliga grunden för kamerabevakningen.

Om bevakningen avser en arbetsplats, ska ett yttrande från ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på arbetsplatsen lämnas in tillsammans med ansökan.

Yttrande av kommunen

12 § Innan tillsynsmyndigheten beslutar om tillstånd till kamerabevakning ska den kommun där bevakningen ska ske få tillfälle att yttra sig, om det av särskild anledning behövs ett yttrande.

Beslut om tillstånd

13 § I ett beslut om tillstånd till kamerabevakning ska det anges vem som ska bedriva bevakningen och i förekommande fall vem som ska ha hand om bevakningen för tillståndshavarens räkning.

Beslutet ska förenas med villkor om hur kamerabevakningen får anordnas. Villkoren ska avse

1. bevakningens ändamål,
2. den utrustning som får användas och var utrustningen får placeras,
3. det område eller typ av område som får bevakas och de tider då bevakning får ske, och
4. upplysning om bevakningen, bevarande eller annan behandling av bilder eller ljud och andra förhållanden som har betydelse för att skydda enskildas personliga integritet, om sådana villkor behövs för tillståndet.

Ett tillstånd får meddelas för en begränsad tid.

Ändrade förhållanden

14 § Om förutsättningarna för ett tillstånd ändras, får tillsynsmyndigheten besluta om nya villkor eller, om förutsättningarna för tillstånd inte längre är uppfyllda, återkalla tillståndet.

Upplysning om kamerabevakning och enskildas rätt till information

Krav på upplysning

15 § Upplysning om kamerabevakning ska lämnas genom tydlig skyltning eller på något annat verksamt sätt.

Om ljud kan avlyssnas eller tas upp vid bevakningen, ska en särskild upplysning lämnas om detta.

Bestämmelser om rätten till information om den personuppgiftsbehandling som kamerabevakningen innebär finns i EU:s dataskyddsförordning och andra föreskrifter som anges i 6 §.

Undantag från upplysningskravet och rätten till information

16 § Upplysning om kamerabevakning och information om den personuppgiftsbehandling som kamerabevakningen innebär behöver inte lämnas vid

1. bevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning,

2. bevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller Säkerhetspolisen, om det av särskild anledning finns risk för allvarlig brottslighet och syftet med bevakningen är att förebygga, förhindra eller upptäcka sådan brottslig verksamhet eller utreda eller lagföra sådana brott,

3. bevakning som sker för att skydda en byggnad, en annan anläggning eller ett område som enligt 4 § 4, 5 § 1–5 eller 6 § första stycket skyddslagen (2010:305) har förklarats vara skyddsobjekt, om bevakningen endast omfattar skyddsobjektet eller ett område i dess omedelbara närhet,

4. bevakning som Försvarsmakten bedriver från ett fordon, fartyg eller luftfartyg som ett led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan bevakning,

5. bevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller den som är räddningsledare enligt lagen (2003:778) om skydd mot olyckor, om bevakningen är av vikt för att avvärja en överhängande fara för olycka, begränsa verkningarna av en inträffad olycka eller minska risken för nya olyckor, och

6. bevakning som bedrivs av den som är räddningsledare enligt lagen om skydd mot olyckor, om bevakningen är av vikt för att efterforska en försvunnen person.

Undantagen i första stycket gäller inte om ljud ska avlyssnas eller tas upp vid kamerabevakningen.

Undantag i enskilda fall

17 § Om det finns synnerliga skäl får tillsynsmyndigheten i enskilda fall besluta om undantag från upplysningskravet och rätten till information om den personuppgiftsbehandling som kamerabevakningen innebär.

Ansökan om undantag

18 § En ansökan om sådant undantag som avses i 17 § ska göras skriftligen hos tillsynsmyndigheten.

Ansökan ska innehålla uppgift om den som ska bedriva kamerabevakningen och i förekommande fall den som ska ha hand om bevakningen för hans eller hennes räkning samt skälen för ansökan.

Om bevakningen avser en arbetsplats, ska ett yttrande från ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på arbetsplatsen lämnas in tillsammans med ansökan.

Yttrande av kommunen

19 § Innan tillsynsmyndigheten beslutar om sådant undantag som avses i 17 §, ska den kommun där kamerabevakningen ska ske få tillfälle att yttra sig, om bevakningen avser en plats dit allmänheten har tillträde och det av särskild anledning behövs ett yttrande.

Beslut om undantag

20 § I ett beslut om undantag enligt 17 § ska det anges vem som ska bedriva kamerabevakningen och i förekommande fall vem som ska ha

hand om bevakningen för hans eller hennes räkning. Beslutet ska förenas med de villkor som behövs och får meddelas för en begränsad tid.

Om förutsättningarna för ett beslut om undantag ändras, får tillsynsmyndigheten besluta om nya villkor eller, om förutsättningarna för ett sådant beslut inte längre är uppfyllda, återkalla beslutet.

Förhandlingsskyldighet för arbetsgivare

21 § I fråga om arbetsgivares beslut om kamerabevakning av en arbetsplats, finns bestämmelser om förhandlingsskyldighet i 11–14 §§ lagen (1976:580) om medbestämmande i arbetslivet.

Tystnadsplikt och utlämnande av uppgifter

22 § Den som tar befattning med en uppgift som har inhämtats genom kamerabevakning får inte obehörigen röja eller utnyttja det som han eller hon på detta sätt har fått veta om någon enskilds personliga förhållanden.

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

Tillsyn, sanktionsavgifter och skadestånd

Tillsynsmyndighet

23 § Den myndighet som regeringen bestämmer utövar tillsyn över kamerabevakning enligt denna lag.

Befogenheter

24 § Bestämmelser om tillsynsmyndighetens befogenheter i EU:s dataskyddsförordning och de föreskrifter som anges i 6 § ska gälla även vid tillsynen över att denna lag följs.

Sanktionsavgifter

25 § Tillsynsmyndigheten får ta ut en sanktionsavgift av den som bedriver kamerabevakning och

1. bryter mot tillståndskravet i 7 §,
2. inte följer villkor i ett beslut om tillstånd som har meddelats med stöd av 13 eller 14 §§,
3. bryter mot upplysningskravet i 15 §, eller
4. inte följer villkor i ett beslut om undantag som har meddelats med stöd av 20 §.

26 § Vid beslut om sanktionsavgift ska artikel 83.1, 83.2 och 83.3 i EU:s dataskyddsförordning, i den ursprungliga lydelsen, och 6 kap. 4–7 §§ lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning tillämpas. Vid kamerabevakning som omfattas av brottsdatalagen (2018:000) ska i stället 6 kap. 3 § tredje stycket och 6 kap. 4–9 §§ den lagen tillämpas.

27 § Vid sådana överträdelser som avses i 25 § 1 och 2 ska avgiftens storlek bestämmas med tillämpning av artikel 83.4 i EU:s dataskyddsförordning, i den ursprungliga lydelsen, eller, i fråga om myndigheter, med tillämpning av den lägre avgiftsnivån i 6 kap. 2 § andra stycket lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning. Vid kamerabevakning som omfattas av brottsdatalagen ska avgiftens storlek i stället bestämmas med tillämpning av 6 kap. 3 § första stycket den lagen.

Vid sådana överträdelser som avses i 25 § 3 och 4 ska avgiftens storlek bestämmas med tillämpning av artikel 83.5 i EU:s dataskyddsförordning, i den ursprungliga lydelsen, eller, i fråga om myndigheter, med tillämpning av den högre avgiftsnivån i 6 kap. 2 § andra stycket lagen med kompletterande bestämmelser till EU:s dataskyddsförordning. Vid kamerabevakning som omfattas av brottsdatalagen ska avgiftens storlek i stället bestämmas med tillämpning av 6 kap. 3 § andra stycket den lagen.

Skadestånd

28 § Vid överträdelse av bestämmelser i denna lag eller av beslut som har meddelats med stöd av lagen ska bestämmelser om rätt till ersättning i artikel 82 i EU:s dataskyddsförordning tillämpas. Vid kamerabevakning som omfattas av brottsdatalagen (2018:000) ska i stället 7 kap. 1 § den lagen tillämpas.

Överklagande

29 § Tillsynsmyndighetens beslut enligt denna lag får överklagas till allmän förvaltningsdomstol. När ett beslut överklagas, är tillsynsmyndigheten motpart i domstolen.

Beslut om tillstånd till kamerabevakning och om undantag enligt 20 § får överklagas även av den kommun där bevakningen ska ske och, om bevakningen ska avse en arbetsplats, av en organisation som företräder arbetstagarna på arbetsplatsen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

---

1. Denna lag träder i kraft den 1 augusti 2018.
2. Genom lagen upphävs kameraövervakningslagen (2013:460).
3. Tillstånd till kameraövervakning som har beslutats enligt den upphävda lagen och som avser kamerabevakning som omfattas av kravet på tillstånd i den nya lagen gäller fortfarande. Övriga tillstånd som har beslutats enligt den upphävda lagen gäller inte längre.
4. Anmälningar som har gjorts enligt den upphävda lagen gäller inte längre.
5. Beslut om undantag från upplysningskravet som har fattats enligt 27 § tredje stycket den upphävda lagen gäller som ett beslut om undantag från upplysningskravet och rätten till information enligt 17 § den nya lagen.
6. Ärenden som har inletts hos länsstyrelserna enligt den upphävda lagen men ännu inte har avgjorts ska överlämnas till den myndighet som utövar tillsyn över kamerabevakning enligt den nya lagen.

7. Om ett beslut som har fattats enligt den upphävda lagen har överklagats av någon annan än tillsynsmyndigheten enligt den nya lagen, är tillsynsmyndigheten motpart i domstolen.

8. Äldre föreskrifter om straff gäller fortfarande för överträdelser som har skett före ikraftträdandet.

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

Härigenom föreskrivs i fråga om offentlighets- och sekretesslagen (2009:400)

dels att 32 kap. 3 § ska ha följande lydelse,

dels att rubriken närmast efter 32 kap. 2 § ska lyda ”Kamerabevakning”.

32 kap.

3 §[1]

Sekretess gäller för sådan uppgift om en enskilds personliga förhållanden som har inhämtats genom *kameraövervakning* som avses i *kameraövervakningslagen (2013:460)*, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men.	Sekretess gäller för sådan uppgift om en enskilds personliga förhållanden som har inhämtats genom *kamerabevakning* som avses i *kamerabevakningslagen (2018:000)*, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men.

Sekretessen enligt första stycket gäller hos en domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

---

1. Denna lag träder i kraft den 1 augusti 2018.
2. Äldre föreskrifter gäller fortfarande för uppgift som har inhämtats före ikraftträdandet.

[1] Senaste lydelse 2013:461

3 Ärendet och dess beredning

Regeringen beslutade den 26 november 2015 att ge en särskild utredare i uppdrag att utreda vissa frågor om kameraövervakning (dir. 2015:125). Det övergripande syftet med utredningen var att säkerställa att kameraövervakning kan användas där det behövs för att bekämpa brott och samtidigt garantera ett starkt skydd för den personliga integriteten.

Den 27 april 2016 utfärdades Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), nedan kallad dataskyddsförordningen. Dataskyddsförordningen, som börjar tillämpas den 25 maj 2018, finns i svensk lydelse i *bilaga 1*. Samtidigt med dataskyddsförordningen antogs Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, nedan kallat det nya dataskyddsdirektivet. Direktivet finns i svensk lydelse i *bilaga 2*.

Genom tilläggsdirektiv den 16 juni 2016 vidgades utredningens uppdrag till att avse en analys av hur regleringen i kameraövervakningslagen (2013:460) bör anpassas till den nya EU-rättsliga dataskyddsregleringen (dir. 2016:54).

Utredningen, som antog namnet Utredningen om kameraövervakning – brottsbekämpning och integritetsskydd (Ju 2015:14), överlämnade i juni 2017 betänkandet En ny kamerabevakningslag (SOU 2017:55). En sammanfattning av betänkandet finns i *bilaga 3*. Utredningens lagförslag finns i *bilaga 4.* Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 5*. Remissvaren finns tillgängliga i Justitiedepartementet (dnr Ju2017/05495/L6).

Riksdagen har tillkännagett att regeringen bör överväga att införa ett undantag från tillståndsplikten när det gäller kameraövervakning av vilt (bet. 2014/15:JuU15 punkt 9, rskr. 2014/15:139). Riksdagen har därefter tillkännagett att regeringen snarast bör gå riksdagens tidigare beslut till mötes och återkomma med ett förslag om att ersätta tillståndsplikten för kameraövervakning med ett anmälningsförfarande (bet. 2016/17:MJU4 punkt 3, rskr. 2016/17:26 och rskr. 2016/17:27). Frågorna behandlas i avsnitt 6.2.

Riksdagen har tillkännagett för regeringen att det är viktigt att åstadkomma en ordning som gör det möjligt för polisen att i större utsträckning än i dag använda kameraövervakning i områden som är utsatta för allvarlig brottsligheten (bet. 2016/17:JuU17 punkt 1, rskr. 2016/17:212). Frågan behandlas i avsnitt 6.

Riksdagen har också tillkännagett för regeringen att polisens tillståndskrav för kameraövervakning ska tas bort och ersättas av en anmälningsplikt senast i samband med att den nya kamerabevakningslagen träder i kraft den 25 maj 2018 (bet. 2017/18:JuU19 punkt 1, rskr 2017/18:127) Frågan behandlas i avsnitt 6.2.

4 Gällande rätt och pågående reformarbete

4.1 Den generella regleringen om skydd för personuppgifter

4.1.1 Europakonventionen och Europarådets dataskyddskonvention

Europakonventionen

Rätten till respekt för den personliga integriteten ingår som en del i rätten till respekt för privatlivet enligt den europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Av artikel 8 i Europakonventionen följer att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. En offentlig myndighet får inte inskränka åtnjutandet av denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.

Europakonventionen är inkorporerad i svensk rätt genom lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna. Av 2 kap. 19 § regeringsformen, förkortad RF, framgår att lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden på grund av Europakonventionen.

Europarådets dataskyddskonvention

Inom Europarådet antogs år 1981 en konvention (nr 108) om skydd för enskilda vid automatisk databehandling av personuppgifter, den s.k. dataskyddskonventionen. Konventionens syfte är att säkerställa den enskildes rätt till personlig integritet i samband med automatiserad behandling av personuppgifter. Regleringen kan ses som en precisering av skyddet enligt artikel 8 i Europakonventionen när det gäller automatiserad behandling av personuppgifter. Samtliga medlemsstater i EU har tillträtt konventionen. Inom Europarådet pågår för närvarande en översyn av konventionen.

4.1.2 EU:s nuvarande dataskyddsreglering

EU:s stadga om de grundläggande rättigheterna

Enligt artikel 6.1 i fördraget om Europeiska unionen ska EU:s stadga om de grundläggande rättigheterna ha samma rättsliga värde som fördragen. I stadgan bekräftas de rättigheter som har sin grund i medlemsstaternas gemensamma författningstraditioner och internationella förpliktelser, Europakonventionen, unionens och Europarådets sociala stadgor samt rättspraxis vid Europeiska unionens domstol och Europeiska domstolen

för de mänskliga rättigheterna. Stadgans huvudsakliga syfte är att kodifiera de grundläggande fri- och rättigheter som EU redan erkänner.

I stadgans artikel 7 föreskrivs, efter förebild i artikel 8 i Europakonventionen, att var och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sin korrespondens. Av artikel 8 följer vidare att var och en har rätt till skydd för personuppgifter. Rättighetens innebörd är att personuppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Vidare har var och en rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. En oberoende myndighet ska kontrollera att dessa regler efterlevs. Av artikel 51 framgår att stadgan riktar sig till medlemsstaterna när de tillämpar unionsrätten.

Enligt artikel 52 måste varje begränsning i utövandet av de fri- och rättigheter som erkänns i stadgan vara föreskriven i lag och vara förenlig med det väsentliga innehållet i dessa fri- och rättigheter. Begränsningar får, med beaktande av proportionalitetsprincipen, göras endast om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors fri- och rättigheter. I den mån en rättighet som erkänns i stadgan motsvarar en rättighet som också garanteras i Europakonventionen ska rättigheten i stadgan ha samma innebörd och räckvidd som i konventionen.

1995 års dataskyddsdirektiv och dataskyddsrambeslutet

Den i nuläget tillämpliga allmänna regleringen inom EU om skydd av personuppgifter finns i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet). Direktivet syftar till att garantera en i alla medlemsstater hög och 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, till exempel allmän säkerhet och försvar samt statens verksamhet på straffrättens område.

Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet) är, som namnet antyder, tillämpligt på informationsutbyte över gränserna. Dataskyddsrambeslutet gäller däremot inte för rent nationell personuppgiftsbehandling inom exempelvis polisens område. Från dataskyddsrambeslutets tillämpningsområde undantas också personuppgiftsbehandling inom området nationell säkerhet. På detta område finns det således inte någon EU-gemensam reglering avseende behandling av personuppgifter.

Både dataskyddsdirektivet och dataskyddsrambeslutet kommer under våren 2018 att ersättas av nya regelverk (se avsnitt 4.2).

4.1.3 Regeringsformen

Av målsättningsstadgandet i 1 kap. 2 § RF framgår att den offentliga makten ska utövas med respekt för den enskilda människans frihet och värdighet samt att det allmänna ska värna den enskildes privatliv och familjeliv. Vidare följer av 2 kap. 6 § andra stycket RF att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, som sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Begränsningar i denna rättighet får endast göras i lag och under de förutsättningar som anges i 2 kap. 21 och 22 §§ RF.

4.1.4 Personuppgiftslagen

Dataskyddsdirektivet har genomförts i svensk rätt huvudsakligen genom personuppgiftslagen (1998:204), förkortad PUL. Bestämmelserna i personuppgiftslagen har till syfte att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter Personuppgiftslagen följer i princip dataskyddsdirektivets struktur och innehåller liksom direktivet bestämmelser om bland annat personuppgiftsansvar, grundläggande krav för behandling av personuppgifter, information till den registrerade, skadestånd och straff.

Personuppgiftslagen är tillämplig även utanför EU-rättens område och gäller både för myndigheter och enskilda som behandlar personuppgifter. Personuppgiftslagen är samtidigt subsidiär, vilket innebär att lagens bestämmelser inte ska tillämpas om det finns avvikande bestämmelser i en annan lag eller förordning. Det finns en stor mängd sådana bestämmelser i sektorsspecifika författningar som främst reglerar hur olika myndigheter får behandla personuppgifter. Det finns också andra typer av författningar med särreglering av viss personuppgiftsbehandling, t.ex. reglerar kameraövervakningslagen viss användning av övervakningskameror och den personuppgiftsbehandling som detta innebär.

4.2 EU:s nya dataskyddsreglering – en betydande reform

4.2.1 Dataskyddsförordningen

Den 27 april 2016 antogs EU:s dataskyddsförordning. Förordningen utgör en ny generell reglering för personuppgiftsbehandling inom EU och ersätter det nuvarande dataskyddsdirektivet från och med den 25 maj 2018. Det huvudsakliga syftet med förordningen är att ytterligare harmonisera och effektivisera skyddet för personuppgifter för att förbättra den inre marknadens funktion och öka enskildas kontroll över sina personuppgifter. Trots att dataskyddsförordningen, till skillnad från dataskyddsdirektivet, är direkt tillämplig innehåller den många bestämmelser som förutsätter eller ger utrymme för kompletterande nationella bestämmelser av olika slag.

Regeringen har den 15 februari 2018 beslutat propositionen Ny dataskyddslag, prop. 2017/18:105. I propositionen föreslås bl.a. att personuppgiftslagen ska upphävas och att de i förhållande till dataskyddsförordningen kompletterande bestämmelser som är av generell karaktär ska samlas i en ny övergripande nationell reglering om dataskydd, lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning, nedan kallad dataskyddslagen. Den nya lagen föreslås träda i kraft den 25 maj 2018.

4.2.2 Ett nytt dataskyddsdirektiv

Samtidigt med dataskyddsförordningen antogs det nya dataskyddsdirektivet som innehåller särregler för sådan personuppgiftsbehandling som behöriga myndigheter utför 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. Direktivet ska vara genomfört i svensk rätt senast den 6 maj 2018.

Utredningen om 2016 års dataskyddsdirektiv (Ju 2016:06) har haft i uppdrag att föreslå hur direktivet ska genomföras i svensk rätt i en ny ramlagstiftning med bestämmelser om skydd av personuppgifter inom direktivets tillämpningsområde (dir. 2016:21). Utredningen lämnade i april 2017 förslag till en sådan lagstiftning, kallad brottsdatalagen, i delbetänkandet Brottsdatalag (SOU 2017:29). Den 4 oktober lämnade utredningen sitt slutbetänkande Brottsdatalag – kompletterande lagstiftning (SOU 2017:74). Slutbetänkandet innehåller bl.a. förslag till de författningsändringar som krävs för att anpassa vissa centrala författningar om rättsväsendets behandling av personuppgifter till de nya förutsättningarna. Regeringen har den 1 mars 2018 beslutat lagrådsremissen Ny brottsdatalag. Brottsdatalagen föreslås träda i kraft den 1 augusti 2018. Slutbetänkandet bereds för närvarande inom Regeringskansliet.

4.3 Kameraövervakningslagen

Särskilda regler för användning av övervakningskameror har funnits i svensk rätt sedan 1977 då lagen (1977:20) om TV-övervakning infördes. Regelverket har därefter setts över ett antal gånger och bl.a. anpassats till EU:s nuvarande dataskyddsdirektiv. Kameraövervakningslagen trädde i kraft den 1 juli 2013. Dessförinnan reglerades kameraövervakning i två lagar: lagen (1998:150) om allmän kameraövervakning och personuppgiftslagen. Syftet med den nya lagen var att modernisera regleringen av kameraövervakning på ett sätt som skulle säkerställa balansen mellan intresset av att använda kameraövervakning för berättigade ändamål och intresset av att skydda den enskildes integritet (propositionen En ny kameraövervakningslag, prop. 2012/13:115).

4.3.1 Definitioner och tillämpningsområde

Kameraövervakningslagen innehåller bestämmelser om kameraövervakning, dvs. användning av övervakningskameror och övrig övervakningsutrustning. Syftet med lagen är att tillgodose behovet av kameraövervakning för berättigade ändamål samtidigt som enskilda skyddas mot otillbörliga intrång i den personliga integriteten (1 §). Lagen gäller i stället för personuppgiftslagen (6 §).

I kameraövervakningslagen finns ett antal definitioner (2 §), däribland av begreppet övervakningskameror. Med övervakningskameror avses enligt lagen tv-kameror, andra optisk-elektroniska instrument och därmed jämförbara utrustningar som är uppsatta så att de, utan att manövreras på platsen, kan användas för personövervakning samt separata tekniska anordningar för avlyssning eller upptagning av ljud vilka i samband med användning av sådan utrustning används för personövervakning.

Kravet att kameran ska vara uppsatt innebär att placeringen av kameran ska ha en viss varaktighet. En kamera som endast används helt kortvarigt är därmed inte en övervakningskamera som omfattas av lagen. Att kameran ska kunna användas utan att manövreras på platsen innebär att den fortlöpande hanteringen av utrustningen inte ska ske på plats. Lagen är alltså inte tillämplig på handhållna kameror. Endast det förhållandet att en kamera sätts i gång på stället eller fungerar med inbyggd automatik innebär inte att den manövreras på platsen och att lagen inte är tillämplig. Med personövervakning avses att personer kan identifieras genom övervakningen. För att en möjlighet till identifiering ska anses föreligga krävs att sådana kännetecken kan iakttas som gör att man utan större osäkerhet kan skilja de personer som iakttas från andra personer. Så är fallet om hela personen eller personens ansikte syns tydligt. Även sådant som utmärkande klädsel, speciella kroppsrörelser eller särskild kroppskonstitution kan möjliggöra identifiering.

Kameraövervakningslagen gäller vid kameraövervakning med övervakningskameror som är uppsatta i Sverige, om den som bedriver övervakningen är etablerad i Sverige eller i tredjeland. Med tredjeland avses en stat som varken ingår i EU eller är ansluten till EES (2 §). Lagen gäller också vid behandling av bild- och ljudmaterial som tagits upp vid sådan övervakning, om behandlingen utförs av den som bedriver övervakningen eller för hans eller hennes räkning (3 §). Lagen gäller dock inte vid kameraövervakning av en plats dit allmänheten inte har tillträde, om övervakningen bedrivs av en fysisk person som ett led i en verksamhet av rent privat natur (5 §). Undantaget kan t.ex. omfatta kameraövervakning i en privatbostad när övervakningen bedrivs av den som bor där. Lagen gäller inte heller vid hemlig kameraövervakning enligt rättegångsbalken eller lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (4 §). Sedan den 1 augusti 2017 är kameraövervakning som sker från obemannade luftfartyg, s.k. drönare, undantagna från lagens tillämpningsområde om övervakningen bedrivs av någon annan än en myndighet (propositionen Kameraövervakningslagen och möjligheterna att använda drönare, prop. 2016/17:182).

4.3.2 Kameraövervakning av platser dit allmänheten har tillträde

Tillståndsplikt som huvudregel

Lagen skiljer mellan kameraövervakning av en plats dit allmänheten har tillträde och kameraövervakning av en plats dit allmänheten inte har tillträde. För kameraövervakning av platser dit allmänheten har tillträde gäller mer detaljerade bestämmelser som bl.a. innebär att det som huvudregel krävs tillstånd för att övervakningen ska vara tillåten (8 §). Denna skiljelinje har funnits sedan lång tid tillbaka och begreppet plats dit allmänheten har tillträde har blivit föremål för en omfattande praxis. Till platser dit allmänheten har tillträde räknas exempelvis gator, torg, parker, butiker, banker, restauranger, biografer och badhus. Även bussar i allmän kommunikation och taxibilar har ansetts vara platser till vilka allmänheten har tillträde. De flesta utrymmen inne i skolor och gemensamhetsutrymmen i flerfamiljshus anses däremot inte vara platser dit allmänheten har tillträde. Detsamma gäller många arbetsplatser (se prop. 2012/13:115 s. 28).

Tillstånd till kameraövervakning ska ges om intresset av sådan övervakning väger tyngre än den enskildes intresse av att inte bli övervakad (9 §). Vid bedömningen av intresset av kameraövervakning ska det särskilt beaktas om övervakningen behövs för att förebygga, avslöja eller utreda brott, förhindra olyckor eller andra därmed jämförliga ändamål. Vid bedömningen av den enskildes intresse av att inte bli övervakad ska det särskilt beaktas hur övervakningen ska utföras, om teknik som främjar skyddet av den enskildes personliga integritet används och vilket område som ska övervakas.

Undantag från tillståndsplikten

Det finns vissa undantag från tillståndsplikten (10 §). Tillstånd krävs inte vid övervakning som sker med en övervakningskamera som för säkerheten i trafiken eller arbetsmiljön är uppsatt på ett fordon, en maskin eller liknande för att förbättra sikten för föraren eller användaren.

Vidare är viss övervakning som bedrivs av Trafikverket tillståndsfri. Det gäller vägtrafikövervakning och övervakning vid betalstationer för trängselskatt och infrastrukturavgifter. Tillstånd krävs inte heller vid trafikövervakning i en vägtunnel som bedrivs av någon annan tunnelhållare än Trafikverket, vid övervakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning eller vid övervakning till skydd för vissa skyddsobjekt. Undantag från tillståndsplikten gäller vidare vid övervakning som Försvarsmakten bedriver från fordon, fartyg eller luftfartyg som ett led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan övervakning.

Slutligen krävs det inte tillstånd vid övervakning i kasinon, om övervakningen har till syfte att förebygga, avslöja eller utreda brott eller lösa tvister om spel mellan spelare och den som anordnar spelet.

Tillfälliga undantag från tillståndsplikten

I några fall får kameraövervakning bedrivas under högst en månad utan att ansökan om tillstånd har gjorts (11 §). Det gäller övervakning som bedrivs av Polismyndigheten eller räddningsledare, om övervakningen är av vikt för att avvärja en hotande olycka eller för att begränsa verkningarna av en inträffad olycka. Det gäller också övervakning som bedrivs av räddningsledare, om övervakningen är av vikt för att efterforska en försvunnen person. Slutligen gäller det övervakning som bedrivs av Polismyndigheten eller Säkerhetspolisen, om det av särskild anledning finns risk för att allvarlig brottslighet som innebär fara för liv eller hälsa eller för omfattande förstörelse av egendom kommer att utövas på en viss plats och syftet med övervakningen är att förebygga eller förhindra brott.

Om ansökan om tillstånd görs inom en månad från det att övervakningen inleds, får övervakningen bedrivas utan tillstånd till dess att ansökningen har prövats.

Kameraövervakning efter anmälan

Kameraövervakning av vissa särskilda platser dit allmänheten har tillträde är tillåten efter endast en anmälan till länsstyrelsen (12–15 §§). För kameraövervakning av dessa platser krävs alltså inte något tillstånd. En övervakningskamera får efter anmälan sättas upp i en banklokal, en lokal hos ett kreditmarknadsföretag eller ett postkontor eller i området omedelbart utanför in- och utgångar till en sådan lokal. Detsamma gäller vid uttagsautomater eller liknande anordningar. Vidare får en övervakningskamera sättas upp efter anmälan i en butikslokal eller i en yta i en butikslokal där det bedrivs bankverksamhet genom ombud eller postverksamhet. Motsvarande gäller för kameraövervakning i en tunnelbanevagn eller av en tunnelbanestation samt i parkeringshus.

Kameraövervakning efter anmälan är dock bara tillåten om vissa särskilt angivna förutsättningar är uppfyllda. Till exempel måste kameraövervakningen ha till enda syfte att förebygga, avslöja eller utreda brott eller, vad gäller övervakning i en tunnelbanevagn eller av en tunnelbanestation, att förhindra olyckor eller begränsa verkningarna av en olycka. För butiker krävs vidare bl.a. att den som avser att bedriva övervakning har ingått en skriftlig överenskommelse om övervakningen med skyddsombudet, skyddskommittén eller en organisation som företräder de anställda på arbetsplatsen.

Ansökan, tillståndsbeslut och anmälan

En ansökan om tillstånd till kameraövervakning ska göras hos länsstyrelsen i det län där övervakningen ska ske (16 §). En ansökan ska innehålla vissa angivna uppgifter (16 och 17 §§) och ett beslut om tillstånd ska förenas med villkor om hur kameraövervakningen får anordnas (19 §). Villkoren ska bl.a. avse övervakningens ändamål och det område som får övervakas. Länsstyrelsen ska också besluta om de övriga villkor som behövs för tillståndet. Sådana villkor får avse upplysningar om övervakningen, upptagning, användning, bevarande eller annan behandling av bilder, avlyssning eller upptagning av ljud samt andra förhållanden som har betydelse för att skydda enskildas personliga integritet. Ett tillstånd får

meddelas för en begränsad tid och får ändras eller återkallas om förutsättningarna för tillståndet ändras eller inte längre är uppfyllda (20 §).

En anmälan om kameraövervakning ska göras hos länsstyrelsen i det län där kameraövervakningen ska ske (21 §). Om de förhållanden som har redovisats i en anmälan ändras, ska länsstyrelsen underrättas om förändringen.

4.3.3 Kameraövervakning av platser dit allmänheten inte har tillträde

För kameraövervakning av platser dit allmänheten inte har tillträde krävs varken tillstånd eller anmälan. Kameraövervakning av sådana platser är tillåten i två olika situationer.

För det första får övervakningen bedrivas, om den som ska övervakas har samtyckt till det (22 §). Med samtycke avses varje slag av frivillig, särskild och otvetydig viljeyttring genom vilken någon, efter att ha fått information, godtar att bli kameraövervakad (2 §). Samtycket behöver inte vara skriftligt och den övervakade har rätt att när som helst återkalla samtycket. Om ett samtycke återkallas får ytterligare övervakning inte ske.

För det andra får sådan kameraövervakning bedrivas utan samtycke, om övervakningen behövs för att förebygga, avslöja eller utreda brott, förhindra olyckor eller för andra berättigade ändamål, och övervakningsintresset väger tyngre än den enskildes intresse av att inte bli övervakad (23 §). Vid denna bedömning ska särskilt beaktas hur övervakningen ska utföras, om teknik som främjar skyddet av den enskildes personliga integritet används och vilket område som ska övervakas. Exempel på andra berättigade ändamål är skolors arbete med att förebygga och förhindra kränkningar av elever samt tillverkningsföretags kontroll av produktionsprocesser (se prop. 2012/13:115 s. 154).

4.3.4 Upplysningsplikt

Vid all kameraövervakning enligt kameraövervakningslagen gäller som huvudregel en upplysningsplikt. Upplysning om kameraövervakning ska lämnas genom tydlig skyltning eller på något annat verksamt sätt (25 §). Upplysning ska också lämnas om vem som bedriver kameraövervakningen, om detta inte framgår av förhållandena på platsen. Om ljud kan avlyssnas eller tas upp vid övervakningen, ska det lämnas en särskild upplysning om detta. Upplysningsplikten inträder när övervakningsutrustningen sätts upp. Den som bedriver övervakningen ska på begäran även informera den övervakade om ändamålet med övervakningen (26 §).

I vissa fall behöver det inte lämnas någon upplysning om kameraövervakningen (27 §). Det gäller bl.a. vid övervakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning och vid övervakning till skydd för vissa skyddsobjekt. Det finns också en möjlighet för länsstyrelsen att medge undantag från upplysningsplikten i enskilda fall, om det finns synnerliga skäl. Undantagen från upplysningsplikten gäller inte övervakning som omfattar avlyssning eller upptagning av ljud.

4.3.5 Behandling av ljud och bildmaterial, tystnadsplikt m.m.

Kameraövervakningslagen innehåller ett antal bestämmelser som närmare reglerar hur bild- och ljudmaterial från kameraövervakning får behandlas. Bestämmelserna innebär bl.a. att den som bedriver kameraövervakning inte får behandla bild- och ljudmaterial från övervakningen för något ändamål som är oförenligt med det som materialet samlades in för (28 §). Dessutom får tillgång till bild- och ljudmaterial från kameraövervakning inte ges till fler personer än vad som behövs för att övervakningen ska kunna bedrivas (29 §).

I kameraövervakningslagen regleras också hur länge bild- och ljudmaterial från kameraövervakning får bevaras (32 §). Material från kameraövervakning av en plats dit allmänheten har tillträde får bevaras under högst två månader, om inte länsstyrelsen beslutar om en längre bevarandetid. Material från övervakning av en plats dit allmänheten saknar tillträde får inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med övervakningen. Om bild- eller ljudmaterial från kameraövervakning används i någon annan verksamhet hos den som bedriver kameraövervakningen, ska i stället regleringen i personuppgiftslagen eller annan författning som gäller för behandling av personuppgifter i den verksamheten, exempelvis polisdatalagen (2010:361), tillämpas (33 §).

I kameraövervakningslagen anges också under vilka förutsättningar det är tillåtet att till tredjeland föra över bild- och ljudmaterial från kameraövervakning som innehåller personuppgifter (34–36 §§). I lagen finns också en bestämmelse om tystnadsplikt och utlämnande av uppgifter (37 §).

4.3.6 Tillsyn

Datainspektionen har det centrala ansvaret för tillsyn enligt kameraövervakningslagen och utövar dessutom den operativa tillsynen över kameraövervakning av platser dit allmänheten inte har tillträde (38 och 40 §§ samt 1 § kameraövervakningsförordningen [2013:463]). I Datainspektionens centrala tillsynsansvar ingår bl.a. att utvärdera rättstillämpningen och ge råd och stöd till länsstyrelserna. Dessa utövar i sin tur den operativa tillsynen över kameraövervakning av platser dit allmänheten har tillträde och ska se till att tillståndskravet och anmälningsplikten för uppsatta övervakningskameror som inte har tagits i bruk följs (39 §).

Tillsynsmyndigheterna får inom ramen för sin tillsynsverksamhet meddela förelägganden, som får förenas med vite (41 och 42 §§). Tillsynsmyndigheterna har också rätt att för tillsynen få tillträde till kontrollrum och andra delar av en övervakningsanläggning samt att få tillgång till och granska bild- eller ljudmaterial (43 §).

4.3.7 Skadestånd, straff och överklagande

Enligt kameraövervakningslagen ska den som bedriver kameraövervakning ersätta den övervakade för skada och kränkning av den personliga integriteten som kameraövervakning i strid med lagen har orsakat (44 §). Ersättningsskyldigheten kan jämkas i den utsträckning det är skäligt, om den som har bedrivit övervakningen visar att felet inte berodde på honom eller henne.

Lagen innehåller också bestämmelser om straff vid vissa överträdelser av lagen (45 §) och om förverkande av övervakningsutrustning (46 §).

Tillsynsmyndigheternas beslut enligt lagen får överklagas till allmän förvaltningsdomstol. Datainspektionen har rätt att överklaga ett beslut om kameraövervakning av en plats dit allmänheten har tillträde. I vissa fall får beslut också överklagas av den kommun där övervakningen ska ske eller, om kameraövervakningen ska avse en arbetsplats, av en organisation som företräder de anställda på arbetsplatsen (47 § och 3 § kameraövervakningsförordningen). Tillsynsmyndigheterna får bestämma att deras beslut ska gälla omedelbart (48 §).

5 En ny kamerabevakningslag

5.1 Ett nytt särskilt regelverk för kamerabevakning

Regeringens förslag: Kameraövervakningslagen ska upphävas och ersättas av en ny lag: kamerabevakningslagen.

I kamerabevakningslagen ska det finnas bestämmelser om kamerabevakning som kompletterar EU:s dataskyddsförordning och genomför EU:s dataskyddsdirektiv. I lagen ska det också finnas bestämmelser om sådan kamerabevakning som inte omfattas av förordningen eller direktivet.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: En stor majoritet av remissinstanserna, bl.a. *Justitiekanslern*, *Kammarrätten i Stockholm*, *Datainspektionen*, *Försvarets Radioanstalt*, *Länsstyrelsen i Östergötlands län*, *Svensk Handel* och *Landsorganisationen i Sverige (LO)*, tillstyrker eller har inga synpunkter på förslaget. *Polismyndigheten* anser att det inte finns några vägande skäl för att ställa upp tillkommande krav på kamerabevakning i en särskild lag eftersom den nya dataskyddsregleringen ändå kommer leda till ett förstärkt skydd för den personliga integriteten. Enligt Polismyndigheten skulle anpassade regler för kamerabevakning i stället kunna införas i annan lagstiftning som reglerar personuppgiftsbehandling.

Skälen för regeringens bedömning

Ett betydande reformbehov

Det kan inledningsvis konstateras att det finns vissa problem med tillämpningen av den nuvarande kameraövervakningslagen. Ett sådant

problem är att rättspraxis har utvecklats på ett sätt som innebär allt för begränsade möjligheter att få tillstånd till kameraövervakning. Det finns vidare en osäkerhet kring hur lagens tillämpningsområde förhåller sig till användning av ny teknik samt brister i efterlevnaden av regleringen vid kameraövervakning på arbetsplatser. Regeringen bedömer därför i likhet med utredningen att den nuvarande lagstiftningen både försvårar en ändamålsenlig användning av kameratekniken och innehåller vissa brister i integritetsskyddet. Det finns därför redan till följd av detta skäl att förändra den svenska regleringen på området.

Kameraövervakning innebär vidare att det i de flesta fall sker en sådan personuppgiftsbehandling som omfattas av den nya EU-rättsliga dataskyddsregleringen, dvs. dataskyddsförordningen eller det nya dataskyddsdirektivet. All nationell reglering av personuppgiftsbehandling måste anpassas till den nya EU-regleringen och för kameraövervakningslagens del kan konstateras att reformbehovet är betydande.

EU-förordningar ska enligt artikel 288 i fördraget om Europeiska unionens funktionssätt ha allmän giltighet och vara till alla delar bindande och direkt tillämpliga i varje medlemsstat. EU-förordningar gäller alltså fullt ut och med samma innehåll inom hela EU och ska inte genomföras i nationell rätt. Bestämmelser om kameraövervakning som upprepar innehållet i dataskyddsförordningen eller som avviker från EU-regleringen kan därför inte behållas eller införas i svensk rätt om inte förordningen lämnar utrymme för det. Det nya dataskyddsdirektivet kräver däremot ett nationellt genomförande. Detta innebär att det inom direktivets tillämpningsområde måste finnas svenska bestämmelser som reglerar den personuppgiftsbehandling som kameraövervakning innebär och som uppfyller direktivets krav.

Mot denna bakgrund gör utredningen bedömningen att många av kameraövervakningslagens bestämmelser antingen måste upphävas eller ändras (se SOU 2017:55 s. 105–166). Så är t.ex. fallet med de definitioner som finns i 2 § kameraövervakningslagen samt bestämmelserna i 8–24 §§ om när kameraövervakning är tillåten.

Regeringen instämmer i utredningens bedömning att det krävs en omfattande reform av den nuvarande svenska regleringen av kameraövervakning för att anpassa den till den nya EU-rättsliga dataskyddsregleringen.

En ny svensk lag om kamerabevakning

Utredningen föreslår att kameraövervakningslagen upphävs och att en ny lag införs. Som utredningen anför skulle ett alternativ till detta kunna vara att inte införa någon särskild reglering för kameraövervakning överhuvudtaget. Ett sådant alternativ skulle innebära att kameraövervakning reglerades helt av de allmänna bestämmelserna om personuppgiftsbehandling i dataskyddsförordningen och dataskyddslagen samt personuppgiftsreglering som genomför det nya dataskyddsdirektivet (framför allt brottsdatalagen). Därutöver finns s.k. särskilda registerförfattningar som reglerar personuppgiftsbehandling inom olika sektorer, både inom och utanför EU-rättens tillämpningsområde.

Trots att dataskyddsförordningen är direkt tillämplig finns emellertid visst utrymme för medlemsstaterna att behålla eller införa särskilda regler för personuppgiftsbehandling. Detta gäller särskilt sådan personuppgiftsbehandling som sker inom den offentliga sektorn. Svensk lagstiftning som kompletterar dataskyddsförordningen kan nämligen med stöd av artikel 6.2 i förordningen innehålla specifika bestämmelser för sådan personuppgiftsbehandling som är nödvändig för att fullgöra en rättslig förpliktelse, utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning. Sådana bestämmelser ska anpassa tillämpningen av bestämmelserna i dataskyddsförordningen genom att fastställa specifika krav för uppgiftsbehandlingen och andra åtgärder för att säkerställa en laglig och rättvis behandling. Enligt artikel 36.5 i dataskyddsförordningen får den nationella rätten dessutom innehålla ett krav på samråd med eller förhandstillstånd av tillsynsmyndigheten i sådana fall. Det är därför möjligt att t.ex. behålla ett tillståndskrav för viss kameraövervakning. Artikel 88 i dataskyddsförordningen ger vidare medlemsstaterna utrymme att behålla eller införa särskild nationell reglering som rör personuppgiftsbehandling i anställningsförhållanden, vilket är av betydelse för kameraövervakning av arbetsplatser. I enlighet med skäl 8 till dataskyddsförordningen kan medlemsstaterna dessutom under vissa förutsättningar och i den utsträckning det är nödvändigt för samstämmigheten och för att göra de nationella bestämmelserna begripliga, införliva delar av förordningen i nationell rätt.

Det nya dataskyddsdirektivet kräver ett nationellt genomförande vilket innebär att det måste finnas en svensk reglering som omfattar kameraövervakning inom direktivets tillämpningsområde, dvs. primärt brottsbekämpande myndigheters kameraövervakning. Nationell reglering kan i enlighet med artikel 1.3 i dataskyddsdirektivet också innehålla starkare skyddsåtgärder än de som följer av direktivet.

Som *Polismyndigheten* påpekar kommer den nya dataskyddsregleringen att innebära förstärkningar av skyddet för den personliga integriteten i olika avseenden. Detta utgör dock enligt regeringens mening inte i sig tillräckliga skäl för att helt avskaffa den svenska regleringen om kameraövervakning. EU-reformen innebär också att regleringen av personuppgiftsbehandling, i vart fall inledningsvis, kommer att upplevas som ett förhållandevis komplext och svårtillämpat rättsområde. Det finns därför goda skäl att behålla en särskilt anpassad svensk reglering för kameraövervakning. En sådan reglering kan både underlätta för förståelsen och innebära möjligheter att snabbt få till stånd en enhetlig och ändamålsenlig rättstillämpning på området.

Regeringen instämmer i utredningens bedömning att reformen med anledning av den nya EU-regleringen är så omfattande att det inte är lämpligt att genomföra den inom ramen för den nuvarande kameraövervakningslagen. Att behålla den nuvarande lagen skulle inte heller på samma sätt som en ny lag tydliggöra att bestämmelserna i stora delar har sin bakgrund i den nya EU-regleringen.

Mot denna bakgrund bör kameraövervakningslagen upphävas och ersättas av en ny svensk lag. Som utredningen anför kan det ifrågasättas om kameraövervakning är ett rättvisande begrepp för den kameraanvändning som bör omfattas av regleringen. Det är fråga om kameraanvändning som sker för berättigade ändamål, t.ex. att skydda

människors liv och hälsa mot brott och olyckor. Sådan kameraanvändning skapar många gånger trygghet för det stora flertalet människor som vistas på de platser där kamerorna används. Ordet övervakning kan dessutom föra tankarna till en kontroll där enskildas intresse av att inte bli föremål för fotografering eller filmning inte har beaktats i tillräcklig utsträckning. Ordet bevakning beskriver, enligt regeringens uppfattning, bättre den kameraanvändning som ska omfattas av lagen. Den nya lagen bör därför benämnas kamerabevakningslagen.

Kamerabevakningslagen kommer att innehålla bestämmelser som kompletterar dataskyddsförordningen och som genomför det nya dataskyddsdirektivet. Detta bör framgå redan av en sådan inledande bestämmelse som regelmässigt tas in i svensk lagstiftning som har unionsrättslig bakgrund. Eftersom lagen även fortsättningsvis bör gälla generellt för kamerabevakning bör det även framgå att bestämmelser i lagen också gäller sådan kamerabevakning som inte omfattas av dataskyddsförordningen eller det nya dataskyddsdirektivet, exempelvis Försvarsmaktens kamerabevakning.

5.2 Utgångspunkter för den nya lagen

5.2.1 Allmänna utgångspunkter

Regeringens bedömning: Kamerabevakningslagens bestämmelser måste vara förenliga med regleringen i EU:s dataskyddsförordning och EU:s dataskyddsdirektiv.

Kamerabevakningslagen bör endast innehålla de bestämmelser som särskilt behövs för kamerabevakning till skillnad mot annan personuppgiftsbehandling. Bestämmelserna bör, så långt det är förenligt med EU-regleringen och ändamålsenligt, vara desamma för all kamerabevakning.

Kamerabevakningslagens bestämmelser bör, i den utsträckning det är lämpligt, utformas på samma sätt som motsvarande bestämmelser i den nuvarande kameraövervakningslagen.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna instämmer i bedömningen eller har inga synpunkter på den.

Skälen för regeringens bedömning: En given utgångspunkt för bestämmelserna i den nya kamerabevakningslagen är att de ska vara förenliga med regleringen i dataskyddsförordningen och det nya dataskyddsdirektivet. Den nya kamerabevakningslagen bör huvudsakligen betraktas som en dataskyddsreglering vilket innebär att den i första hand bör innehålla regler om behandling av personuppgifter i samband med kamerabevakning.

Till skillnad mot kameraövervakningslagen kan inte kamerabevakningslagen innehålla en uttömmande reglering av den personuppgiftsbehandling som kamerabevakningen innebär. Tvärtom innebär en anpassning till EU:s nya dataskyddsreglering att allmänna principer och generella bestämmelser i sådana regelverk måste eller bör gälla

även vid kamerabevakning. En annan utgångspunkt för kamerabevakningslagen bör därför vara att den endast ska innehålla de bestämmelser som särskilt behövs för kamerabevakning. Kamerabevakningslagen bör alltså inte innehålla bestämmelser som i princip skulle utgöra upprepningar av vad som annars gäller för personuppgiftsbehandling. Däremot kan regleringen av begriplighetsskäl behöva hänvisa till vissa andra bestämmelser för att tydliggöra vad som gäller vid kamerabevakning.

De bestämmelser som tas in i kamerabevakningslagen bör, så långt det är förenligt med EU-regleringen och ändamålsenligt, vara desamma för all kamerabevakning, oavsett om den omfattas av dataskyddsförordningen, det nya dataskyddsdirektivet eller helt faller utanför EU-rättens tillämpningsområde. Detta för att bestämmelserna ska bli så förutsebara och enkla att tillämpa som möjligt.

Bestämmelserna i den nya lagen bör dessutom, i den utsträckning det är lämpligt, utformas på samma sätt som motsvarande bestämmelser i dagens kameraövervakningslag.

5.2.2 Ökade möjligheter till kamerabevakning och ett förstärkt integritetsskydd

Regeringens bedömning: Kamerabevakningslagen bör ge ökade möjligheter till kamerabevakning. Samtidigt bör lagen leda till ett förstärkt skydd för den personliga integriteten, särskilt vid kamerabevakning på arbetsplatser.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: En majoritet av remissinstanserna, däribland *Tullverket*, *Stockholms stad*, *Kristinehamns kommun*, *Sveriges Kommuner och Landsting*, *Jernhusen*, *Svensk Handel* och *Svensk kollektivtrafik*, ställer sig bakom bedömningen eller har inga synpunkter på den. *Justitiekanslern* konstaterar att det är möjligt att öka möjligheterna till kamerabevakning för berättigade syften utan att det skapar en obalans i förhållande till skyddet för den personliga integriteten och anser att förslagen i stort ger uttryck för en välavvägd syn på förhållandet mellan kamerabevakning och personlig integritet.

Skälen för regeringens bedömning

Ny teknik innebär både nya möjligheter och risker

Kameratekniken har länge använts i många olika samhälleliga syften. Två särskilt viktiga syften är att bekämpa brott och förhindra olyckor. Andra betydelsefulla användningsområden för tekniken är kopplade till t.ex. arbetslivet, sjukvården, jord- och skogsbruk eller miljön. Den tekniska utvecklingen medför dessutom att kameratekniken kan användas för nya berättigade ändamål. Det är angeläget att lagstiftningen inte hindrar en sådan berättigad användning av modern teknik.

Den snabba tekniska utvecklingen kan även medföra särskilda integritetsrisker. Kameror kan t.ex. göras allt mindre och svårare att upptäcka. Vidare kan kameror som monteras på en drönare eller byggs in i annan rörlig teknik göra det svårt för enskilda att värja sig mot obefogad

övervakning. Utvecklingen av ny teknik kan samtidigt skapa bättre möjligheter att begränsa onödiga integritetsintrång. Med inbyggd integritetsfrämjande teknik kan exempelvis bildmaterial maskeras automatiskt så att det inte är möjligt att identifiera personer i bildmaterialet, om detta inte behövs. Vissa kameror kan också ställas in för att aktiveras först efter olika typer av larm, onormala rörelsemönster eller särskilda ljud som skottlossning eller glaskross. Genom den nya EU-rättsliga dataskyddsregleringen slås dessutom viktiga principer om inbyggt dataskydd och dataskydd som standard fast (artikel 25 i dataskyddsförordningen och artikel 20 i det nya dataskyddsdirektivet). Detta innebär bl.a. att den som behandlar personuppgifter ska genomföra och integrera lämpliga tekniska åtgärder för att skydda de registrerades rättigheter och t.ex. se till att inte fler personuppgifter behandlas än vad som är nödvändigt med hänsyn till ändamålet.

Ett viktigt verktyg vid brottsbekämpning

Kamerabevakning kan vara särskilt betydelsefull i de brottsbekämpande myndigheternas verksamhet. På offentliga platser kan tekniken fungera som ett viktigt komplement till andra brottsförebyggande åtgärder. Kamerabevakning kan också underlätta avslöjandet av pågående brott och vara av avgörande betydelse i efterföljande utredningar. En effektiv brottsbekämpning bidrar i sin tur till ett tryggare samhälle. På senare tid har det blivit tydligt att det finns ett ökat behov och efterfrågan av kamerabevakning i samhället för brottsbekämpande och trygghetsskapande ändamål. Det är angeläget att lagstiftningen inte ställer upp för höga krav för exempelvis Polismyndighetens eller kommunernas möjligheter att vid behov använda tekniken som ett led i att skapa trygga offentliga miljöer.

Regeringen beslutade i mars 2017 skrivelsen Tillsammans mot brott – Ett nationellt brottsförebyggande program (skr. 2016/17:126). Programmet är en del av en större satsning på brottsförebyggande arbete och berör allt från individinriktade insatser till förebyggande åtgärder mot situationer eller platser där risken för brott är hög. Ett exempel på en sådan insats är användningen av kamerabevakning.

I juni 2017 presenterade Polismyndigheten en rapport med sin nationella lägesbild över utsatta områden i landet där det finns en sådan kriminell närvaro som medför otrygghet för både invånare och näringsidkare (dnr: HD 44/14A203.023/2016). Av rapporten framgår bl.a. att polisen de senaste åren har ökat sin närvaro i dessa områden, tillsatt kommun- och områdespoliser samt genomfört riktade insatser och medborgardialoger. Ett trygghetsskapande arbete pågår också, t.ex. samarbete med lokaltrafiken och bostadsbolagen, trygghetsvandringar där den fysiska miljön kontrolleras, nattvandringar och sociala insatsgrupper. Det råder enligt regeringens bedömning inget tvivel om att kamerabevakning också kan vara ett viktigt verktyg i detta arbete. Vidare startade Polismyndigheten i januari 2017 ett kameraprojekt vars syfte är att skapa nationella riktlinjer och metoder för kameraanvändningen, bygga upp ett nationellt och enhetligt kameraövervakningssystem och stödja de olika regionerna med kompetens och utrustning för kameraövervakning.

Under senare år har flera terrorangrepp skett i länder i vår närhet, bl.a. i Frankrike, Belgien, Tyskland och Storbritannien. Mot denna bakgrund har regeringen tagit fram en nationell strategi mot terrorism som ska vara utgångspunkten för Sveriges långsiktiga arbete på detta område både nationellt och internationellt (skr. 2014/15:146). Syftet med strategin är att skapa en tydlig struktur för det arbete som krävs för att motverka terroristbrottslighet. Vikten av samverkan mellan olika aktörer betonas i strategin. Vidare slås fast att terrorism bl.a. riktar sig mot offentliga platser som platser för kollektivtrafik och kultur- och köpcentra och att även tillfälliga arrangemang som idrotts- och kulturevenemang har visat sig vara tänkbara mål för terroristattentat. Som utredningen framhåller har kamerabevakning på sådana platser i flera fall bidragit till att brotten har kunnat utredas och att terroristerna och deras medhjälpare har kunnat identifieras och lagföras.

I april 2017 riktades också ett terrorangrepp mot centrala Stockholm där även ett tidigare terrordåd skett. Vid angreppet dödades och skadades ett flertal människor. Den 7 juni 2017 träffade regeringen och Moderaterna, Centerpartiet, Liberalerna och Kristdemokraterna en överenskommelse om åtgärder mot terrorism. I överenskommelsen anges att om den då pågående utredningen om kameraövervakning inte skulle resultera i en tillräcklig förbättring ur polisens perspektiv ska det finnas beredskap från regeringen att agera. Bland annat mot denna bakgrund beslutade regeringen den 13 december 2017 att ge en särskild utredare i uppdrag att föreslå åtgärder som kan underlätta kameraövervakning som sker i brottsbekämpande syfte (dir. 2017:124). Syftet med utredningen är att säkerställa att myndigheternas möjlighet att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda brott och att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, ska vara flexibel och verksamhetsanpassad. Utredaren ska även analysera förutsättningarna för kameraövervakning av allmänna transportmedel och stationer. Uppdraget som rör förenkling av möjligheterna till kameraövervakning i brottsbekämpande syfte och därmed sammanhängande frågor ska redovisas senast den 15 augusti 2018 och uppdraget som avser kameraövervakning av allmänna transportmedel och stationer ska redovisas senast den 15 februari 2019.

Behoven att använda kamerabevakning tillgodoses inte i dag

Genom den kartläggning som utredningen har gjort är det enligt regeringens mening tydligt att behovet av att kunna använda kamerabevakning inte tillgodoses av den nuvarande lagen och gällande praxis. För att tillstånd till kamerabevakning med inspelning ska beviljas krävs t.ex. enligt etablerad praxis normalt att den aktuella platsen kan anses vara särskilt brottsutsatt. Att visa detta kräver ofta utförlig dokumentation från sökanden om att allvarlig eller omfattande brottslighet redan har inträffat på platsen, vilket kan vara svårt och mycket tidsödande att få fram. Ibland krävs det dessutom att sökanden presenterar dokumentation av brottsligheten på andra platser än den som ska bevakas som ett slags jämförelsematerial (jfr t.ex. Kammarrätten i Stockholms dom 2016-06-09 i mål nr 7392–15).

Vissa platser är vidare inte, eller kan inte visas vara, frekvent utsatta för brott men löper likväl på grund av generella hotbilder en särskild risk att utsättas för brott jämfört med andra platser i samhället. Som exempel kan nämnas lokaler och platser som används av religiösa samfund, asylboenden eller medieredaktioner. På platser med nybyggnation där det på goda grunder kan antas finnas en särskild risk för brottslighet är det också i regel omöjligt att på förhand visa platsens utsatthet för brott.

Det står vidare klart att rättspraxis är alltför restriktiv för kommuner som vill använda kamerabevakning i trygghetsskapande syften. Även om uppgiften att bekämpa och lagföra brott i första hand är en fråga för Polismyndigheten och andra brottsbekämpande myndigheter, finns numera en uttalad ambition att stärka samverkan mellan rättsväsendets myndigheter och andra aktörer såsom kommuner, landsting och andra i det civila samhället vad gäller bl.a. brottsförebyggande arbete (se bl.a. skr. 2016/17:126 s. 24–31). Vidare har, som utredningen anför, kommuner ett visst eget ansvar för allmän ordning och säkerhet inom kommunen i enlighet med regleringen i ordningslagen (1993:1632). Även andra aktörer kan ha ett starkt intresse av att motverka brott genom egna åtgärder för att säkerställa att deras verksamheter kan bedrivas utan störningar och för att skydda personal och besökare. Det kan gälla exempelvis på platser som akutmottagningar på sjukhus och väntrum hos myndigheter. För dessa kan kamerabevakning vara ett bra komplement till andra åtgärder. Kamerabevakning kan direkt avskräcka personer från att begå brott på platsen och öka den upplevda tryggheten för dem som vistas där. Detta kan i sin tur öka den sociala kontrollen på platsen. Material från kamerabevakning kan också vara av avgörande betydelse vid utredningen av begångna brott.

Inte heller finns det i dag tydliga möjligheter att kamerabevaka för att motverka brottslighet riktad mot vissa särskilt utsatta fordon eller personer som använder dessa, såsom räddningsfordon och brandmän eller polisbilar och polismän. Kamerabevakning kan också ha en viktig roll att spela för att skydda jordbruks- och skogsbruksmaskiner. Sådan egendom representerar höga värden och är stöldbegärlig. Egendomen måste ofta lämnas obevakad, inte sällan ute i skog och mark.

Enligt regeringens bedömning kan möjligheterna till kamerabevakning för berättigade syften öka utan att det leder till en obalans i förhållande till skyddet för den personliga integriteten. Denna uppfattning får stöd av bl.a. *Justitiekanslern*. Mot den bakgrunden bör en utgångspunkt för den nya lagen vara att ge ökade möjligheter till kamerabevakning.

Integritetsskyddet på arbetsplatser bör förstärkas

Samtidigt som en ny reglering bör ge ökade möjligheter till kamerabevakning finns också anledning att överväga åtgärder som leder till förstärkningar av integritetsskyddet. Regeringen vill här särskilt framhålla att kamerabevakning på arbetsplatser kan innebära betydande risker för anställdas personliga integritet. Detta har tydliggjorts bl.a. genom Integritetskommitténs (Ju 2014:09) kartläggning (SOU 2016:41 s. 232–241) och ett antal tillsynsbeslut från Datainspektionen på senare år (se t.ex. beslut 2015-12-16, dnr 351–2015). Det har i dessa sammanhang framkommit att informationen till de anställda ofta är bristfällig och att det

förekommit fall där övervakningen använts för att kontrollera hur de anställda arbetar. Som en ytterligare utgångspunkt för kamerabevakningslagen bör därför gälla att lagen ska leda till ett förstärkt skydd för den personliga integriteten, särskilt vid kamerabevakning på arbetsplatser.

5.3 Lagens syfte, tillämpningsområde och förhållandet till andra bestämmelser

5.3.1 Lagens syfte

Regeringens förslag: Syftet med kamerabevakningslagen ska vara att tillgodose behovet av kamerabevakning för berättigade ändamål och att skydda fysiska personer mot otillbörliga intrång i den personliga integriteten vid sådan bevakning.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Datainspektionen* föreslår att syftesbestämmelsen utgår eftersom den får ett otydligt förhållande till syftesbestämmelserna i dataskyddsförordningen och brottsdatalagen. Övriga remissinstanser tillstyrker eller har inga synpunkter på förslaget.

Skälen för regeringens förslag: I enlighet med vad *Datainspektionen* påpekar kommer syftesbestämmelserna i dataskyddsförordningen respektive brottsdatalagen att gälla när bestämmelser i dessa regelverk tillämpas, även i fråga om sådan personuppgiftsbehandling som utgör kamerabevakning. Kamerabevakningslagen kommer dock att innehålla vissa bestämmelser som kompletterar dataskyddsförordningen, genomför det nya dataskyddsdirektivet och reglerar vad som gäller för sådan kamerabevakning som inte omfattas av EU-regleringen. Enligt regeringens mening kan en syftesbestämmelse i den nya lagen vara värdefull, bl.a. för att ge vägledning för tolkningen av de materiella bestämmelser som ska gälla särskilt vid kamerabevakning. Regeringen instämmer också i utredningens bedömning att varken dataskyddsförordningen eller övrig personuppgiftsreglering hindrar en syftesbestämmelse med den föreslagna utformningen.

Kamerabevakningslagen bör därför, i likhet med den nuvarande kameraövervakningslagen, innehålla en bestämmelse som anger att syftet med lagen är att tillgodose behovet av kamerabevakning för berättigade ändamål och att skydda fysiska personer mot otillbörliga intrång i den personliga integriteten vid sådan bevakning.

5.3.2 Lagens förhållande till annan dataskyddsreglering

Regeringens förslag: Utöver vad som föreskrivs i kamerabevakningslagen ska följande reglering gälla:

1. EU:s dataskyddsförordning, dataskyddslagen, föreskrifter som har meddelats i anslutning till den lagen och andra föreskrifter som kompletterar EU:s dataskyddsförordning.

2. Brottsdatalagen, föreskrifter som har meddelats i anslutning till den lagen och andra föreskrifter som genomför EU:s dataskyddsdirektiv.

3. Föreskrifter om sådan behandling av personuppgifter som inte omfattas av dataskyddsförordningens eller brottsdatalagens tillämpningsområde.

Regeringens bedömning: Kamerabevakningslagen behöver inte innehålla någon särskild bestämmelse om att de uttryck som används i lagen har samma innebörd som i annan tillämplig personuppgiftsreglering.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningens förslag innehåller ingen hänvisning till föreskrifter som inte omfattas av dataskyddsförordningens eller brottsdatalagens tillämpningsområde. Utredningen föreslår en bestämmelse om att de uttryck som används i kamerabevakningslagen ska ha samma betydelse som i dataskyddsförordningen för sådan kamerabevakning som omfattas av förordningen eller dataskyddslagen, eller som i brottsdatalagen när det gäller kamerabevakning som omfattas av den lagen.

Remissinstanserna: Majoriteten av remissinstanserna, bl.a. *Justitiekanslern* och *Förvaltningsrätten i Jönköping*, tillstyrker förslaget eller har inga synpunkter på det. Justitiekanslern anför att även om överskådligheten i den nya lagen påverkas är den valda metoden att föredra framför alternativet att enbart reglera kamerabevakning genom de generella personuppgiftslagarna. Några remissinstanser, däribland *Förvaltningsrätten i Umeå*, påpekar att de olika regelverkens inbördes förhållande blir svårtillgängligt och att det kan bli svårt för enskilda och myndigheter att ta reda på vad som gäller. *Datainspektionen* anser att den föreslagna bestämmelsen om kamerabevakningslagens förhållande till andra bestämmelser är otydlig och att det inte framgår av lagtexten hur lagen förhåller sig till s.k. registerförfattningar som ibland kan innehålla bestämmelser som ska tillämpas vid kamerabevakning. Enligt *Säkerhetspolisen* bör det övervägas om den föreslagna bestämmelsen av tydlighetsskäl också bör innehålla en hänvisning till kommande lagstiftning om personuppgiftsbehandling i Säkerhetspolisens brottsbekämpande verksamhet som rör nationell säkerhet.

Skälen för regeringens bedömning: Kamerabevakningslagen bör som konstateras i avsnitt 5.2.1 endast innehålla de bestämmelser som särskilt behövs för kamerabevakning i förhållande till annan personuppgiftsbehandling. Regeringen föreslår i enlighet med denna utgångspunkt endast ett fåtal materiella bestämmelser i lagen (se avsnitt 6 och 7). Dessa bestämmelser får, precis som regleringen i den nuvarande kameraövervakningslagen, en ställning som lex specialis i förhållande till annan nationell personuppgiftsreglering. I övrigt bör tillämpliga bestämmelser i andra personuppgiftsregleringar gälla.

För enskilda är det främst dataskyddsförordningen och den kompletterande regleringen i dataskyddslagen som kommer att tillämpas. För myndigheter och andra offentliga organ handlar det också om sådana särregleringar inom respektive verksamhetsområde som finns i särskilda registerförfattningar. För myndigheter med verksamhet inom det nya dataskyddsdirektivets tillämpningsområde aktualiseras i första hand

brottsdatalagen och annan sektors- eller myndighetsspecifik reglering som genomför direktivet.

När det gäller området utanför EU-rättens tillämpningsområde kan konstateras att 1 kap. 2 § i förslaget till dataskyddslag innehåller en bestämmelse som innebär att dataskyddsförordningen ska gälla även vid behandling av personuppgifter som utgör ett led i en verksamhet som omfattas av unionsrätten och i verksamhet som inte omfattas av avdelning V kapitel 2 i fördraget om Europeiska unionen. Samtidigt föreslås att denna utvidgning av förordningens tillämpningsområde inte ska gälla verksamhet som omfattas av lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet. Utvidgningen ska enligt förslaget inte heller gälla sådan verksamhet som omfattas av 6 kap. polisdatalagen som reglerar Säkerhetspolisens personuppgiftsbehandling i brottsbekämpande verksamhet. Vidare föreslås dataskyddslagen innehålla vissa övergångsbestämmelser som bl.a. innebär att personuppgiftslagen ska fortsätta att gälla i sådan verksamhet hos Försvarsmakten, Försvarets radioanstalt och Totalförsvarets rekryteringsmyndighet som inte omfattas av unionsrätten samt vid sådan behandling av personuppgifter som avses i artikel 2.2 d i dataskyddsförordningen, i den ursprungliga lydelsen.

För att klargöra och, i den mån det behövs, reglera kamerabevakningslagens förhållande till annan reglering om behandling av personuppgifter bör en heltäckande bestämmelse om detta tas in i kamerabevakningslagen. Regeringen anser till skillnad från *Datainspektionen* att den av utredningen föreslagna bestämmelsen på ett tillräckligt tydligt sätt klargör förhållandet till annan reglering på dataskyddsområdet. Som *Säkerhetspolisen* anför finns det dock anledning att förtydliga förhållandet mellan författningar som reglerar personuppgiftsbehandling utanför EU-rättens tillämpningsområde och kamerabevakningslagen. Det bör därför framgå direkt av kamerabevakningslagen att föreskrifter som rör personuppgiftsbehandling som inte omfattas av dataskyddsförordningens eller brottsdatalagens tillämpningsområde också gäller i tillämpliga delar.

I vissa fall kommer bestämmelser i kamerabevakningslagen innehålla hänvisningar till dataskyddsförordningen, främst av upplysande karaktär. Sådana hänvisningar i lagen bör som utgångspunkt vara dynamiska, precis som motsvarande hänvisningar i förslaget till dataskyddslag. Hänvisningarna kommer således att omfatta även eventuella framtida ändringar i dataskyddsförordningen vilket får anses nödvändigt för att undvika osäkerhet eller omotiverade avvikelser på området för kamerabevakning. Vissa hänvisningar bör dock i stället vara statiska, dvs. avse dataskyddsförordningen i den ursprungliga lydelsen (se avsnitt 11.2).

Sammanfattningsvis bör det av kamerabevakningslagen framgå att utöver vad som föreskrivs i lagen gäller 1) dataskyddsförordningen, dataskyddslagen, föreskrifter som har meddelats i anslutning till den lagen och andra föreskrifter som kompletterar dataskyddsförordningen, 2) brottsdatalagen, föreskrifter som har meddelats i anslutning till den lagen och andra föreskrifter som genomför dataskyddsdirektivet, och 3)

föreskrifter som rör personuppgiftsbehandling som inte omfattas av dataskyddsförordningens eller brottsdatalagens tillämpningsområde.

Att vissa begrepp i kamerabevakningslagen, exempelvis begreppet behandling, har samma innebörd som i annan tillämplig personuppgiftsreglering följer redan av lagens förhållande till sådan reglering. Till skillnad mot utredningen anser regeringen därför inte att kamerabevakningslagen bör innehålla en särskild bestämmelse om att de uttryck som används i lagen har samma innebörd som i dataskyddsförordningen respektive brottsdatalagen.

5.3.3 Begreppet kamerabevakning

Regeringens förslag: Med kamerabevakning ska avses

1. att en tv-kamera, ett annat optisk-elektroniskt instrument eller en därmed jämförbar utrustning, utan att manövreras på platsen, används på ett sätt som innebär varaktig eller regelbundet upprepad personbevakning,
2. att en separat teknisk anordning för avlyssning eller upptagning av ljud används i samband med sådan användning av utrustning som avses i 1, eller
3. att en separat teknisk anordning används för att behandla bild- och ljudmaterial som tagits upp med sådan utrustning som avses i 1 eller 2.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår att definitionen av begreppet kamerabevakning ska ta sikte på utrustning som används varaktigt eller regelbundet upprepat för personbevakning.

Remissinstanserna: Majoriteten av remissinstanserna tillstyrker förslaget eller har inga synpunkter på det. Ett antal remissinstanser, däribland *Polismyndigheten*, *Ekobrottsmyndigheten* och *Sveriges Kommuner och Landsting*, anser att lagstiftningen borde utformas mer teknikneutralt för att undvika nuvarande och framtida gränsdragningsproblem. *Säkerhet för Näringsliv & Samhälle* framför liknande synpunkter, med hänvisning framför allt till användningen av begreppet utan att manövreras på platsen. *Kustbevakningen* ser vissa gränsdragningsproblem med förslaget, bl.a. vad som gäller i de fall när ett fartyg eller ett luftfartyg fritt kan välja färdväg samt om en kamera som är uppsatt i en del av fartyget men manövreras från en annan del av fartyget omfattas av begreppet utan att manövreras på platsen. Polismyndigheten invänder mot uttalanden av utredningen som skulle kunna innebära att vissa kroppsburna kameror kan omfattas av lagens tillämpningsområde. *Utredningen om självkörande fordon på väg (N 2015:07)* anser att fordonsmonterade kameror som är avsedda att kunna övervaka och framföra ett fordon på väg på ett säkert sätt uttryckligen bör undantas från kamerabevakningslagens tillämpningsområde. *Länsstyrelsen i Uppsala län* anser att fotografering med drönare ska undantas från lagens tillämpningsområde och framhåller att många tillstånd till kameraövervakning med drönare i dag innehåller villkor om att bilder på människor ska raderas eller att kameran bara får aktiveras på sådan höjd att identifiering av människor inte är möjlig. Enligt *Datainspektionen*

knyts det föreslagna tillämpningsområdet åtminstone språkligt till avsikten att använda kameran för att bevaka personer. Det finns enligt Datainspektionen en risk att den som avser kamerabevaka i annat syfte, till exempel för kontroll av växande grödor eller inspektion av tak, kan få uppfattningen att den inte omfattas av kamerabevakningslagen, något som utredningen enligt Datainspektionen inte har avsett. *Förvaltningsrätten i Stockholm* lämnar liknande synpunkter och framhåller att kamerabevakning som skulle kunna medföra personbevakning utan att så faktiskt sker inte längre synes omfattas av tillämpningsområdet. *Sveriges Byggindustrier* anser att det är oklart huruvida drönare som används inom byggbranschen omfattas av lagens tillämpningsområde med hänsyn till att det ofta inte är fråga om varaktig kamerabevakning och önskar förtydliganden i denna del. Ett antal remissinstanser, däribland *Länsstyrelsen i Dalarna* och *Länsstyrelsen i Skåne län*, anser att tidpunkten för när lagen blir tillämplig, liksom tidigare, bör vara när kameran sätts upp eftersom den nu föreslagna ordningen riskerar att leda till bevisproblem vid tillsyn. Även Datainspektionen uppmärksammar att det finns sådana risker men anser samtidigt att det inte längre framstår som motiverat att koppla tillämpningsområdet till uppsättningen av en kamera, mot bakgrund av att kamerabevakning till största delen kommer att regleras som övrig personuppgiftsbehandling. *SJ AB* ställer sig positivt till att lagen föreslås bli tillämplig först i samband med att kameran används eftersom kameror då kan installeras på tåg i samband med tillverkningen och man i ett senare skede kan ta ställning till var och när de ska användas. *Totalförsvarets forskningsinstitut* föreslår att begreppet optisk-elektroniskt instrument byts ut mot optoelektroniska instrument.

Skälen för regeringens bedömning

Nuvarande reglering och praxis

Definitionen av vad som är en övervakningskamera har i väsentliga delar varit densamma sedan den första lagstiftningen på området infördes på 1970-talet. Lagstiftningen har sedan dess omfattat både bevakning med kameror som monterats på fasta platser, t.ex. på eller i byggnader eller på stolpar, och bevakning med kameror som monterats på eller i rörliga objekt, t.ex. fordon. Användning av handhållna kameror, dvs. kameraanvändning från rörliga subjekt, har däremot inte omfattats. Kameraövervakning av avgränsade och bestämda platser var ursprungligen vanligast förekommande och kom därför av naturliga skäl att stå i fokus för lagstiftningen. Även senare lagstiftning på området har dock i huvudsak haft samma fokus, trots att den tekniska utvecklingen inneburit att kameraanvändning från rörliga objekt fortlöpande har ökat.

Kameraövervakningslagen är tillämplig på kameror som är uppsatta så att de utan att manövreras på platsen kan användas för personövervakning (2 §). Genom två avgöranden från Högsta förvaltningsdomstolen (HFD 2016 ref. 71) har viktiga klargöranden skett av hur denna reglering ska tolkas när det gäller kameror som är uppsatta på rörliga objekt. Enligt Högsta förvaltningsdomstolens avgöranden är kameraövervakningslagen som huvudregel tillämplig på kamerautrustade drönare men inte på kameror som placerats i vindrutan på en bil eller på ett cykelstyre. Denna skillnad beror på att kameran på en drönare normalt manövreras från en

plats som är klart åtskild från den där kameran är uppsatt medan kameran i vindrutan på en bil eller på ett cykelstyre är uppsatt i förarens omedelbara närhet.

Med anledning av att framför allt enskilda kunde förväntas få svårt att få tillstånd till kameraövervakning med drönare även för godtagbara ändamål infördes ett undantag från kameraövervakningslagens tillämpningsområde för andra än myndigheters användning av drönare den 1 augusti 2017 (5 a §). Sådan användning av drönare regleras därmed i dag, precis som exempelvis handhållna kameror, av bestämmelserna i personuppgiftslagen i stället.

Ett snävare och mer teknikneutralt tillämpningsområde

Regeringen instämmer i vad bl.a. *Polismyndigheten* och *Sveriges Kommuner och Landsting* anför om att en mer teknikneutral reglering bör eftersträvas för att undvika onödiga gränsdragningsproblem och för att regleringen även ska kunna tillämpas på framtida teknikanvändning. Det kan vidare konstateras att sådan användning av kamerateknik som sker inom dataskyddsförordningens tillämpningsområde huvudsakligen kommer att styras av regleringen i förordningen, vilket i sig innebär ett omfattande och förstärkt integritetsskydd för enskilda. Detta talar för att begreppet kamerabevakning endast bör omfatta sådan kameraanvändning som typiskt sett innebär att det sker en personuppgiftsbehandling. Ett något snävare och mer teknikneutralt tillämpningsområde för den nya lagen bör alltså eftersträvas.

Begreppet utan att manövreras på platsen bör behållas…

Även fortsättningsvis bör en skillnad göras i lagstiftningen mellan kameror som finns i användarens omedelbara närhet, exempelvis handhållna kameror, och kameror som hanteras fortlöpande från en annan plats. Som framgår ovan och som bl.a. *Säkerhet för Näringsliv & Samhälle* påpekar har det i vart fall tidigare funnits vissa praktiska svårigheter att avgöra om viss ny teknik är att anse som manövrerad på platsen eller inte. De domstolsavgöranden som redovisas ovan har dock inneburit viktiga klargöranden. Även om vissa tolkningssvårigheter kan finnas kvar om avgränsningen behålls kan sådana med största sannolikhet inte undgås helt genom att en ny typ av avgränsning införs i stället. Regeringen delar därför utredningens uppfattning att begreppet utan att manövreras på platsen bör behållas i den nya lagen.

Innebörden av att utrustningen används utan att manövreras på platsen bör liksom tidigare vara att den fortlöpande hanteringen sker på ett ställe som är klart åtskilt från den plats där utrustningen finns. Utrustning som fjärrstyrs eller fungerar med inbyggd automatik kan därför i normalfallet inte anses vara manövrerad på platsen. Utrustning som däremot finns i användarens omedelbara närhet och som fortlöpande styrs eller kan styras av användaren är att anse som manövrerad på platsen. Det innebär bl.a. att handhållna kameror inte omfattas av lagens tillämpningsområde och inte heller webbkameror, kameror på stativ eller liknande så länge användaren befinner sig i anslutning till kameran.

När det gäller kameror som på annat sätt bärs på kroppen gör regeringen bedömningen att sådana kameror inte bör omfattas av lagens

tillämpningsområde. Detta gäller även om en sådan kamera innehåller funktioner som gör att den kan fjärrstyras från en annan plats och bärs av en person som är skyldig att lyda order.

I fråga om kameror som sätts upp på eller i fordon, fartyg eller luftfartyg kan, som *Kustbevakningen* uppmärksammar, vissa gränsdragningsfrågor ändå uppkomma. I ljuset av Högsta förvaltningsdomstolens uttalanden i ovan nämnda avgöranden måste emellertid en kamera som fortlöpande hanteras i direkt anslutning till förarplatsen, t.ex. en kamera placerad i vindrutan, anses vara manövrerad på platsen. Dessa kameror omfattas därmed inte av lagens tillämpningsområde. En bedömning måste dock göras från fall till fall och för exempelvis större fartyg kan det vara så att en kamera placeras och riktas på ett sätt som gör att den inte kan anses hanteras fortlöpande på platsen där utrustningen finns.

Det saknas underlag att inom ramen för detta lagstiftningsärende införa ett särskilt undantag från tillämpningsområdet för vissa fordonsmonterade kameror på det sätt som *Utredningen om självkörande fordon på väg (N 2015:07)* efterfrågar. Även om kamerabevakningslagen skulle kunna vara tillämplig på teknik som används i självkörande fordon bör framhållas att lagens tillståndskrav i normalfallet inte gäller för privatpersoner eller företag (se avsnitt 6.2). Frågan om ett undantag från tillståndskravet bör göras för självkörande fordon i övriga fall, dvs. för myndigheter och andra som utför uppgifter av allmänt intresse, behandlas i avsnitt 6.5.

… men den faktiska användningen av tekniken ska vara avgörande

Regeringen instämmer i utredningens bedömning att den nya lagen bör vara tillämplig på sådan kamerabevakning som sker från såväl fasta objekt, t.ex. från byggnader, som från rörliga objekt, t.ex. olika typer av fordon. Att helt undanta kamerabevakning från exempelvis fordon skulle innebära att lagen lätt kan kringgås och även innebära en avsevärd förändring av vad som hittills har gällt och fungerat förhållandevis väl. En sådan avgränsning skulle inte heller ligga i linje med strävan att göra den nya regleringen mer teknikneutral än den nuvarande. Det finns därför inte heller skäl att helt undanta kamerautrustade drönare från lagstiftningens tillämpningsområde, något som bl.a. *Länsstyrelsen i Uppsala* förespråkar. En mer teknikneutral reglering bör i stället åstadkommas genom att lagstiftningen anpassas till övrig personuppgiftsreglering och att fokus läggs på den faktiska användningen av tekniken och de integritetsrisker som denna medför.

Regeringen instämmer därför i utredningens bedömning att lagens tillämplighet inte bör kopplas till att en kamera är uppsatt så att den kan användas för personövervakning. Avgörande bör i stället vara hur kameran faktiskt används. Enligt utredningens förslag ska kamerabevakningslagen gälla när utrustningen används varaktigt eller regelbundet upprepat för personbevakning.

Som bl.a. *Länsstyrelsen i Dalarna* påpekar kan visserligen en sådan ordning tänkas innebära vissa bevissvårigheter för tillsynsmyndigheten genom invändningar om att en uppsatt kamera inte har varit påslagen. Som *Datainspektionen* anför bör dock hänsyn tas till att övrig personuppgiftsreglering är tillämplig endast vid en faktisk behandling av personuppgifter. Någon personuppgiftsbehandling sker inte om en kamera

i och för sig är uppsatt men inte används. De bevissvårigheter som kan uppstå ska heller inte överdrivas. Som utredningen konstaterar bör det i många fall vara uppenbart att utrustningen används, särskilt om inspelning sker. Eftersom den nya lagens tillståndskrav begränsas till att avse myndigheter och privata subjekt som utför uppgifter av allmänt intresse (se avsnitt 6.2) bör sådana invändningar som vissa av länsstyrelserna befarar dessutom bli tämligen sällsynta.

Mot denna bakgrund anser regeringen att beskrivningen av begreppet kamerabevakning i huvudsak bör utformas i enlighet med utredningens förslag. Som Datainspektionen anför kan utredningens föreslagna bestämmelse emellertid leda tanken till att själva syftet med kameraanvändningen är avgörande för lagens tillämpningsområde. För att undvika detta bör bestämmelsen formuleras något annorlunda och ta sikte på sådan utrustning som används på ett sätt som innebär varaktig eller regelbundet upprepad personbevakning. Enligt regeringen framstår det också som mer naturligt att kravet på varaktighet eller regelbunden upprepning tar sikte på personbevakningen och inte, som utredningen föreslår, användningen av utrustningen i sig. Det kommer därmed också stå klart att sådan kameraanvändning som skulle kunna medföra personbevakning utan att så faktiskt sker inte omfattas av tillämpningsområdet. Detta innebär att lagstiftningen får ett snävare och mer teknikneutralt tillämpningsområde än vad som gäller i dag. Ett sådant tillämpningsområde kommer dessutom att harmoniera bättre med övrig personuppgiftsreglering.

Begreppet personbevakning bör ges motsvarande innebörd som begreppet personövervakning i kameraövervakningslagen. Med detta avses att människor kan identifieras genom bevakningen. För att en möjlighet till identifiering ska anses föreligga krävs att sådana kännetecken kan iakttas som gör att man utan större osäkerhet kan skilja de personer som iakttas från andra personer. Så är t.ex. fallet om hela personen eller personens ansikte syns tydligt. Även sådant som utmärkande klädsel, speciella kroppsrörelser eller särskild kroppskonstitution kan dock möjliggöra identifiering. Som utredningen konstaterar är begreppet personbevakning snävare än begreppet personuppgiftsbehandling. Detta innebär exempelvis att kameror som används i parkeringshus enbart för att läsa av bilars registreringsnummer inte omfattas av lagens tillämpningsområde.

Kamerabevakning kan vara varaktig även om den sker vid ett enstaka tillfälle. Vad som är att anse som varaktig personbevakning måste avgöras från fall till fall. Det är emellertid klart att det är fråga om varaktig personbevakning om en kamera under en längre tid är placerad på eller riktad mot en plats där människor normalt vistas, exempelvis på ett torg, i en butik, i ett väntrum eller i en buss.

Helt kortvarig personbevakning, där en enstaka identifierbar människa av en tillfällighet råkar passera i kamerans upptagningsområde, bör däremot inte anses som varaktig. Om detta sker vid ett flertal tillfällen som ligger relativt nära varandra i tiden eller om det av något annat skäl är fråga om systematisk användning av bevakningsutrustning bör personbevakningen dock anses ske med sådan regelbunden upprepning att den ändå omfattas av lagens tillämpningsområde. Därmed omfattas exempelvis sådana rörliga kameror som riktas ut från ett fordon eller är

monterade på en drönare av lagens tillämpningsområde, om användningen innebär att människor regelbundet passerar i kamerans upptagningsområde på ett sätt som gör dem möjliga att identifiera. Även utplacering och användning av kameror på platser där människor passerar mer sällan men med viss regelbundenhet, exempelvis i närheten av en gångstig i skogen, omfattas av lagens tillämpningsområde. Om kameran används på ett sätt som endast innebär enstaka fall av helt kortvarig personbevakning bör lagen dock inte vara tillämplig. Så kan t.ex. vara fallet med kameror som används på svårtillgängliga platser i utomhusmiljöer eller som placerats för att kontrollera en industriell tillverkningsprocess i vars närhet människor normalt inte ska befinna sig, även om någon vid ett enstaka tillfälle kan råka göra det.

I praktiken innebär detta att både sådan kameraanvändning som sker med det direkta syftet att bevaka människor och sådan användning som sker för andra syften men där människor under en längre tid eller någorlunda regelbundet kommer in i kamerans upptagningsområde, omfattas av lagens tillämpningsområde.

Det tillämpningsområde som nu föreslås minskar behovet av sådana undantag i lagstiftningen för exempelvis kamerautrustade drönare, som förespråkas av bl.a. *Länsstyrelsen i Uppsala*. Huruvida lagen är tillämplig på en kamerautrustad drönare eller inte kommer nämligen till skillnad mot i dag att avgöras av hur tekniken faktiskt används. Om drönaren används på ett sätt som innebär varaktig eller regelbundet upprepad personbevakning omfattas den av lagens tillämpningsområde, oavsett vad syftet med användningen är. I vilken utsträckning lagens tillståndskrav och kravet på upplysning ska gälla vid sådan användning diskuteras i avsnitt 6.5 och 7.2. Kamerabevakningslagen blir dock inte tillämplig om drönaren används i andra syften än att bevaka personer, exempelvis för olika typer av mätningar eller besiktningar, om användaren ser till att personer varken varaktigt eller regelbundet upprepat fångas av kameran på ett sätt som gör dem möjliga att identifiera. Det kan exempelvis ske genom att kameran endast är påslagen på viss höjd eller vid flygningar över områden där människor normalt inte uppehåller sig. I enlighet med vad som sägs ovan blir lagen inte heller tillämplig om enstaka identifierbara personer helt kortvarigt hamnar i kamerans upptagningsområde, så länge det inte sker regelbundet.

Det nya tillämpningsområdet

Det saknas anledning att, som *Totalförsvarets forskningsinstitut* föreslår, frångå användningen av begreppet optisk-elektroniskt instrument, eftersom det inte har framkommit några problem vid tillämpningen av det begreppet i kameraövervakningslagen. Som utredningen anför kommer den nya lagen, precis som kameraövervakningslagen, formellt att vara tillämplig också på analog kamerabevakning.

Betydelsen av att också låta kamerabevakningslagen gälla i de fall en separat teknisk anordning används för att behandla upptaget bild- och ljudmaterial kommer att minska med anledning av att sådan behandling i allt väsentligt kommer att styras av annan personuppgiftsreglering. Ett tillståndsbeslut skulle dock kunna innehålla vissa villkor som avser efterföljande behandling av inspelat material vilket innebär att

tillämpningsområdet för kamerabevakningslagen formellt även bör omfatta sådana behandlingar.

Med kamerabevakning ska alltså avses att en tv-kamera, ett annat optisk-elektroniskt instrument eller en därmed jämförbar utrustning, utan att manövreras på platsen, används på ett sätt som innebär varaktig eller regelbundet upprepad personbevakning. Med kamerabevakning ska också avses att en separat teknisk anordning för avlyssning eller upptagning av ljud används i samband med sådan användning av utrustning och att en separat teknisk anordning för att behandla upptaget bild- och ljudmaterial används.

5.3.4 Lagens territoriella tillämpningsområde

Regeringens förslag: Kamerabevakningslagen ska gälla endast om kamerabevakning sker med utrustning som finns i Sverige och den som bedriver bevakningen är etablerad i Sverige eller i tredjeland, samt vid behandling av material som tagits upp med hjälp av sådana kameror. Det senare bör gälla oavsett om behandlingen utförs av den som bedriver bevakningen eller för hans eller hennes räkning.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna tillstyrker eller har inga synpunkter på förslaget.

Skälen för regeringens förslag: Kameraövervakningslagen gäller vid kameraövervakning som sker med övervakningskameror som är uppsatta i Sverige, om den som bedriver övervakningen är etablerad i Sverige eller i tredjeland (3 § första stycket 1). Begreppet övervakningskameror omfattar inte separata tekniska anordningar för att behandla upptaget bild- och ljudmaterial. Användning av sådan utrustning utgör dock också kameraövervakning enligt lagen. I kameraövervakningslagen anges därför att lagen gäller även vid behandling av material som tagits upp vid övervakning med övervakningskameror uppsatta i Sverige, om behandlingen utförs av den som bedriver övervakningen eller för hans eller hennes räkning (3 § första stycket 2).

Dataskyddsförordningens territoriella tillämpningsområde är av naturliga skäl utformat ur ett unionsperspektiv eftersom förordningen ska gälla direkt i alla medlemsstater inom EU. I dataskyddsförordningen regleras alltså inte det territoriella tillämpningsområdet för den nationella lagstiftning som kompletterar dataskyddsförordningen. Det territoriella tillämpningsområdet framgår inte heller uttryckligen av det nya dataskyddsdirektivet men kan sägas följa indirekt av att direktivets materiella tillämpningsområde tar sikte på behandling av personuppgifter som utförs av behöriga myndigheter för vissa särskilda ändamål.

Som framgår i avsnitt 4.2.1 är utgångspunkten att bestämmelserna i kamerabevakningslagen ska utformas på ett gemensamt sätt för all kamerabevakning. Bestämmelser om lagens territoriella tillämpningsområde kan som utredningen framhåller utformas på det sättet utan hinder av EU-regleringen.

Som framgår av föregående avsnitt bör begreppet uppsatt inte överföras till kamerabevakningslagen. I enlighet med utredningens förslag bör regleringen ändå utformas så att den på samma sätt som tidigare träffar

användning av kameror och annan därmed jämförbar utrustning, samt separata tekniska anordningar för avlyssning eller upptagning av ljud, när utrustningen finns i Sverige. Med Sverige avses, i likhet med vad som gäller enligt kameraövervakningslagen, svenskt landterritorium och sjöterritorium samt luftrummet ovanför land- och sjöterritorierna. På samma sätt bör behandling av material som tagits upp vid sådan bevakning omfattas av lagen, oavsett var anordningen för behandling finns, så länge behandlingen utförs av samma juridiska eller fysiska person som bedriver bevakningen eller för hans eller hennes räkning. Vad gäller sådan behandling kommer visserligen lagens bestämmelser i första hand ta sikte på det initiala skedet av behandlingen, dvs. själva upptagningen av bildmaterial. Emellertid skulle exempelvis ett tillståndsbeslut kunna innehålla vissa villkor som avser efterföljande behandling av inspelat material vilket innebär att det territoriella tillämpningsområdet formellt även fortsättningsvis bör omfatta sådana behandlingar.

En ytterligare fråga är om kamerabevakningslagen, liksom kameraövervakningslagen, endast bör gälla när den som bedriver bevakningen är etablerad i Sverige eller i ett tredjeland. Den som är etablerad i ett annat EU-land än Sverige och som bedriver kamerabevakning här skulle då inte omfattas av lagens bestämmelser. Skälet till motsvarande begränsning av kameraövervakningslagens tillämpningsområde är att det ansetts oförenligt med det nuvarande dataskyddsdirektivet att den svenska regleringen även skulle omfatta den som är etablerad i en annan EU-stat (se prop. 2012/13:115 s. 40–41).

Etableringslandsprincipen, som innebär att de föreskrifter som gäller där den personuppgiftsansvarige är etablerad ska tillämpas, kan sägas vara utgångspunkten i dataskyddsförordningens reglering om det territoriella tillämpningsområdet (artikel 3.1 och 3.3). Mot denna bakgrund har den principen även valts som huvudregel i förslaget till dataskyddslag (1 kap. 5 §). Det nya dataskyddsdirektivet avser vidare särskilda verksamheter i en stat, t.ex. brottsbekämpning, som i regel bedrivs på den egna statens territorium, även om det finns ett internationellt polisiärt samarbete som innebär att tjänstemän från en stat under vissa förutsättningar kan agera på en annan stats territorium. Också i verksamheter som inte omfattas av unionsrätten, såsom militär verksamhet, förekommer samarbete som innebär att utländska myndigheter från andra EU-stater kan agera på svenskt territorium.

Enligt regeringens mening bör samma grundprincip gälla för kamerabevakningslagens territoriella tillämpningsområde som för den allmänna regleringen i dataskyddslagen. Kamerabevakningslagen kommer endast innehålla ett fåtal materiella bestämmelser, bl.a. ett begränsat tillståndskrav för vissa subjekt. Det går därför inte att se några konsekvenser som är svåra att acceptera, vare sig från integritets- eller konkurrensperspektiv, med att låta etableringsprincipen fortsätta att gälla också på detta område.

Mot denna bakgrund bör kamerabevakningslagen gälla endast om kamerabevakning sker med utrustning som finns i Sverige och den som bedriver bevakningen är etablerad i Sverige eller i tredjeland, samt vid behandling av material som tagits upp med hjälp av sådana kameror.

5.3.5 Undantag från lagens tillämpningsområde

Regeringens förslag: Kamerabevakningslagen ska inte gälla vid

1. kamerabevakning som en fysisk person utför som ett led i en verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll,
2. hemlig kameraövervakning enligt 27 kap. rättegångsbalken eller lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott,
3. kamerabevakning som sker i en verksamhet som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen, eller
4. kamerabevakning som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: En majoritet av remissinstanserna tillstyrker eller har inga synpunkter på förslaget. *Solna tingsrätt* understryker vikten av att gränsdragningen mellan polisens befogenheter att bedriva kamerabevakning i förebyggande syfte och sådan hemlig kameraövervakning som prövas av allmän domstol tryggas i lagstiftningen. *Ekobrottsmyndigheten* anser att det bör göras tydligare om kameraanvändning i vid bemärkelse vid polisverksamhet ska vara tillståndspliktig enligt den nya lagen, kräva beslut enligt 27 kap. 20 a § rättegångsbalken eller fortsatt vara oreglerad. *Tullverket* har förståelse för utredningens ställningstaganden men framför ändå önskemål om att utreda och reglera spaningsmetoder som t.ex. går ut på att en kamera placeras ut på ett visst avstånd från det objekt som man vill spana på genom kameran. *Datainspektionen* framhåller att det inte är möjligt att införa en bestämmelse i nationell rätt som ger svenska grundlagsbestämmelser företräde framför EU-rätt. Även om det inte är tillfredsställande att frågan om förhållandet till grundlagarna är oklar på kamerabevakningsområdet bör enligt Datainspektionen därför de generella undantagen för grundlagarna och journalistiska ändamål m.m. utgå. *Falu tingsrätt* anser också att det av integritetsskäl kan ifrågasättas varför journalistisk verksamhet ska undantas i den utsträckning som föreslås. *Sveriges television AB* och *Svenska Journalistförbundet* välkomnar dock undantagen och tillstyrker förslaget i denna del. *Länsstyrelsen i Uppsala län* saknar ett resonemang om vad som gäller om en myndighet använder kamerabevakning i sin verksamhet (t.ex. tillsyn med hjälp av drönare) och bilder som tas från denna bevakning skett i en verksamhet som ska anses omfattas av tryckfrihetsförordningen. *Luleå tekniska universitet* anser att formuleringen akademiskt, konstnärligt eller litterärt skapande skapar oklarhet kring lagens tillämpningsområde och undrar bl.a. om undantaget ska gälla också utbildning och forskning vid myndighet. *Malmö kommun* framför liknande synpunkter och efterfrågar tydligare definitioner.

Skälen för regeringens förslag

Privat kamerabevakning

Av artikel 2.2 c i dataskyddsförordningen följer att förordningen inte ska tillämpas på behandling av personuppgifter som en fysisk person utför som

ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll. Något motsvarande undantag finns inte i det nya dataskyddsdirektivet eftersom det primärt reglerar vissa myndigheters behandling av personuppgifter för bl.a. brottsbekämpande ändamål.

Från kameraövervakningslagens tillämpningsområde undantas i dag övervakning av platser dit allmänheten inte har tillträde, om övervakningen bedrivs av en fysisk person som ett led i en verksamhet av rent privat natur (5 §). Att ta in en motsvarande typ av bestämmelse i den nya kamerabevakningslagen skulle visserligen innebära en upprepning av motsvarande undantag i dataskyddsförordningen. Eftersom det kan anses vara nödvändigt för att göra kamerabevakningslagens tillämpningsområde begripligt är det dock fråga om ett sådant införlivande av dataskyddsförordningen i svensk lagstiftning som är tillåtet enligt skäl 8 till förordningen.

Bestämmelsen bör som utredningen föreslår utformas i överrensstämmelse med dataskyddsförordningens undantag. Kamerabevakningslagen bör alltså innehålla en bestämmelse om att lagen inte gäller vid kamerabevakning som en fysisk person utför som ett led i en verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll.

EU-domstolen har prövat innebörden av motsvarande undantag i det nuvarande dataskyddsdirektivet (EU-domstolens dom Ryneš, C-212/13, EU:C:2014:2428). Enligt EU-domstolen kan videoövervakning som delvis omfattar ett område dit allmänheten har tillträde och som därmed går utanför uppgiftshanterarens privata sfär inte anses vara av rent privat natur eller ha samband med hans eller hennes hushåll i den mening som avses i undantaget. Detta innebär att undantaget är begränsat till kamerabevakning av platser dit allmänheten inte har tillträde, utan att det behöver anges uttryckligen i bestämmelsen.

Hemlig kameraövervakning

Hemlig kameraövervakning enligt 27 kap. rättegångsbalken eller lagen om åtgärder för att förhindra vissa särskilt allvarliga brott är undantagen från kameraövervakningslagens tillämpningsområde (4 §). Som flera remissinstanser, däribland *Solna tingsrätt*, påpekar är det angeläget att upprätthålla en tydlig distinktion mellan denna typ av dold kameraövervakning och sådan öppen kamerabevakning som den nu aktuella regleringen bör omfatta. Enligt regeringens mening är den nuvarande avgränsningen i kameraövervakningslagen tydlig och bör användas även i den nya lagen.

Kamerabevakningslagen bör alltså innehålla en bestämmelse om att lagen inte gäller vid hemlig kameraövervakning enligt 27 kap. rättegångsbalken eller lagen om åtgärder för att förhindra vissa särskilt allvarliga brott.

En särskild fråga är hur man ska se på möjligheten för exempelvis Polismyndigheten eller Säkerhetspolisen att använda en spaningsmetod som innebär att en kamera placeras på ett visst ställe och sedan styrs av en polisman på visst avstånd från spaningsobjektet. Detta kan ske både på underrättelsestadiet och på förundersökningsstadiet. *Ekobrottsmyndigheten* och *Tullverket* uttrycker önskemål om tydligare

reglering för denna typ av spaningsmetoder. Det har tidigare övervägts att införa sådan lagstiftning, men så har ännu inte skett (se bl.a. propositionen Åtgärder för att utreda vissa samhällsfarliga brott m.m., prop. 2007/08:163 och SOU 2010:103). Spaningsmetoderna har heller inte varit föremål för närmare överväganden av utredningen och det finns således inte underlag att behandla frågan i detta lagstiftningsärende.

Kamerabevakning i en verksamhet som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen

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

Regleringen i dataskyddsförordningen av förhållandet till yttrande- och informationsfriheten har en motsvarighet i det nuvarande dataskyddsdirektivet som har genomförts i svensk rätt genom 7 § PUL. Artikel 85 i dataskyddsförordningen ger enligt sin ordalydelse ett något större utrymme för undantag än det som finns i direktivet, bl.a. på det sättet att det inte längre föreskrivs att behandling ska ske uteslutande för journalistiska ändamål för att undantag ska kunna göras. Dessutom uttalas i skäl 153 till förordningen att begreppet yttrandefrihet ska ges en bred tolkning.

I den nuvarande kameraövervakningslagen saknas en motsvarighet till den beskrivna regleringen i personuppgiftslagen. Frågan om förhållandet mellan bestämmelser om kameraövervakning och bestämmelserna i tryckfrihetsförordningen och yttrandefrihetsgrundlagen har inte heller diskuterats närmare i tidigare lagstiftningssammanhang. Viss osäkerhet råder därför i frågan. Som utredningen anför har det under senare tid exempelvis uppkommit frågor om de traditionella mediernas användning av kameror på drönare eller kameror monterade på visst sätt för nyhetsrapportering omfattas av kameraövervakningslagens bestämmelser, t.ex. om tillståndsplikt.

Tryckfrihetsförordningen och yttrandefrihetsgrundlagen hindrar i och för sig inte att det i vanlig lag finns bestämmelser som reglerar själva sättet på vilket ett anskaffande av information sker, t.ex. bestämmelser om straffansvar eller om krav på tillstånd, så länge regleringen inte tar sikte på innehållet som sådant, inte ens delvis. Å andra sidan finns ett nära samband mellan själva insamlingen av bilder och ljud och den information som utgörs av bilderna och ljudet. Inte sällan sker publiceringen av bilder och ljud i grundlagsskyddade medier i princip i samma stund som insamlingen sker.

Sveriges detaljerade tryck- och yttrandefrihetsgrundlagar är unika i jämförelse med hur motsvarande reglering ser ut i övriga Europa. Som bl.a. *Sveriges television AB* framhåller är det angeläget att komma till rätta

med den osäkerhet som funnits kring möjligheterna att använda kameratekniken på det grundlagsreglerade området eftersom det kan påverka vitala delar av opinionsskapande verksamhet. Upplysningsbestämmelsen i 7 § första stycket PUL bedömdes förenlig med det nuvarande dataskyddsdirektivets likartade bestämmelser vid införandet av personuppgiftslagen (propositionen Personuppgiftslag, prop. 1997/98:144 och konstitutionsutskottets betänkande, 1997/98:KU18). Som framgår ovan finns det enligt dataskyddsförordningen ett något större utrymme att göra undantag med hänsyn till yttrande- och informationsfriheten än enligt det nuvarande dataskyddsdirektivet. I dataskyddslagen föreslås en bestämmelse om att dataskyddsförordningen och den lagen inte ska tillämpas i den utsträckning det skulle strida mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen (1 kap 7 § första stycket).

Mot denna bakgrund anser regeringen, till skillnad från Datainspektionen, att det är möjligt att införa en bestämmelse i kamerabevakningslagen av det aktuella slaget för det grundlagsskyddade området. Ett sådant undantag bör endast omfatta kamerabevakning som sker inom ramen för verksamhet som skyddas genom tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Som exempel kan nämnas direktsändning av ett sportevenemang med kameror uppsatta på drönare. Däremot bör undantaget inte vara tillämpligt om t.ex. en medieredaktion bedriver kamerabevakning utanför den grundlagsreglerade verksamheten, t.ex. för att skydda sina lokaler eller anställda.

Kamerabevakningslagen bör alltså innehålla en bestämmelse som anger att lagen inte gäller vid kamerabevakning som sker i en verksamhet som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Med anledning av de frågor som *Länsstyrelsen i Uppsala län* väcker bör framhållas att det torde vara mycket ovanligt att myndigheter bedriver kamerabevakning i en verksamhet som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. I sådana fall har precis som i övriga fall grundlagsregleringen företräde.

Kamerabevakning som i andra fall sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande

I 7 § andra stycket PUL finns ett undantag från merparten av lagens bestämmelser för sådan personuppgiftsbehandling som sker uteslutande för journalistiska ändamål eller konstnärligt eller litterärt skapande. Bestämmelsen rör sådana förfaranden som faller utanför tryckfrihetsförordningens och yttrandefrihetsgrundlagens tillämpningsområde. Någon motsvarande bestämmelse finns däremot inte i kameraövervakningslagen.

Som konstateras ovan ska medlemsstaterna enligt artikel 85.2 i dataskyddsförordningen göra vissa undantag från förordningen i sin nationella reglering för behandling som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande. Undantag får dock bara göras om de är nödvändiga för att förena rätten till integritet med yttrande- och informationsfriheten. Samma krav på nödvändighet finns i det nuvarande dataskyddsdirektivet.

Även i denna del innehåller förslaget till dataskyddslag en bestämmelse som motsvarar den som finns i personuppgiftslagen. Enligt 1 kap. 7 § andra stycket förslaget till dataskyddslag ska bestämmelserna i kapitel II och III, artiklarna 24–30 och 35–43 och kapitel V i dataskyddsförordningen inte tillämpas på behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande. Dessutom föreslås att delar av dataskyddslagen (kap. 2–5) inte heller ska vara tillämplig i sådana fall. Vissa av förordningens bestämmelser kommer dock att vara tillämpliga, exempelvis vissa bestämmelser i kapitel IV om säkerhet vid behandling av personuppgifter, bestämmelserna i kapitel VI om tillsyn och kapitel VIII som innehåller regler om rättsmedel, ansvar och sanktioner.

Enligt *Falu tingsrätt* kan det ifrågasättas om kamerabevakningslagen bör innehålla ett så omfattande undantag för journalistisk verksamhet som utredningen föreslår. I detta sammanhang bör framhållas att kamerabevakningslagen endast kommer innehålla ett mindre antal bestämmelser och att det i stället är dataskyddsförordningen som i stor utsträckning kommer att styra vilken kamerabevakning som är tillåten inom förordningens tillämpningsområde. Som framgår ovan innebär förslaget till dataskyddslag vidare att en betydande del av den materiella regleringen i dataskyddsförordningen inte ska tillämpas på sådan personuppgiftsbehandling som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande. Det är angeläget att regleringen håller väl samman och det saknas anledning att låta den begränsade regleringen i kamerabevakningslagen vara tillämplig i situationer då den grundläggande regleringen i dataskyddsförordningen inte är det.

Kamerabevakningslagen bör alltså innehålla en bestämmelse om att lagen inte gäller vid kamerabevakning som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

Innebörden av begreppen journalistiska ändamål respektive akademiskt, konstnärligt eller litterärt skapande måste i första hand avgöras genom en tolkning av dataskyddsförordningen. Några särskilda definitioner av dessa begrepp, som bl.a. *Malmö kommun* efterfrågar, bör därför inte införas i kamerabevakningslagen. Viss ledning bör kunna hämtas från tidigare tillämpning av 7 § andra stycket PUL. Begreppet akademiskt skapande är dock nytt även i EU-regleringen och definieras inte närmare där. Som regeringen anför i propositionen Ny dataskyddslag torde det i vart fall ha en annan betydelse än begreppen utbildning och forskning, bl.a. eftersom forskning är särreglerat på annat sätt i dataskyddsförordningen (se prop. 2017/18:105 s.44–45). Sannolikt har undantaget för akademiskt skapande en förhållandevis liten praktisk betydelse på området för kamerabevakning.

6 Ett begränsat tillståndskrav

6.1 Inget generellt tillståndskrav i den nya lagen

Regeringens bedömning: Kamerabevakningslagen kan inte innehålla ett generellt tillståndskrav eftersom kamerabevakning inom tillämpningsområdet för EU:s dataskyddsförordning endast delvis kan omfattas av ett sådant krav. Inte heller kan ett krav på anmälan av det slag som finns i kameraövervakningslagen behållas generellt. Kamerabevakningslagen kan innehålla ett tillståndskrav för sådan kamerabevakning som omfattas av EU:s dataskyddsdirektiv eller faller utanför EU-regleringens tillämpningsområde.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna instämmer i eller har inga invändningar mot bedömningen.

Skälen för regeringens bedömning

Bakgrunden till dagens tillståndskrav

Det nuvarande kravet på förhandstillstånd för kameraövervakning av platser som allmänheten har tillträde till har funnits länge i svensk rätt. Skälen till att ett sådant krav ursprungligen ställdes upp var att den tekniska utvecklingen inneburit att användning av kamerautrustning för övervakning blivit allt vanligare och att det knappast fanns något skydd mot att utrustningen användes för personövervakning på ett sätt som kränkte enskildas personliga integritet (se proposition om TV-övervakning, prop. 1975/76:194 s. 14–20). Det som då pekades ut var bl.a. kameraövervakning inom sjukvården och kriminalvården samt polisbevakning på centralstationen och tunnelbanan i Stockholm. Vidare uttalades att sådan övervakning gjorde det möjligt att samla in en stor mängd information om enskilda och kunde medföra en särskild risk från integritetssynpunkt om medborgarna mer allmänt blev föremål för denna.

Sedan dess har förhållandena ändrats. Kameraövervakning har blivit betydligt vanligare i samhället samtidigt som regelverken till skydd för enskildas personliga integritet har förstärkts. Genom den nya EU-rättsliga dataskyddsregleringen förstärks integritetsskyddet ytterligare, bl.a. vad gäller enskildas rättigheter och genom en kraftfullare tillsyn. Den nya EU-regleringen innehåller i sig inget krav på förhandstillstånd men möjliggör för medlemsstaterna att i den nationella rätten införa sådana krav för viss personuppgiftsbehandling.

Kamerabevakning inom dataskyddsförordningens tillämpningsområde

Enligt dataskyddsförordningen måste all behandling av personuppgifter vila på en rättslig grund. För att personuppgiftsbehandling ska vara tillåten krävs enligt artikel 6.1 i dataskyddsförordningen att 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.

c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

d) Behandlingen är nödvändig för att skydda intressen 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.

Kamerabevakning enligt kamerabevakningslagen innebär en behandling av personuppgifter. Den som vill kamerabevaka inom dataskyddsförordningens tillämpningsområde måste därför kunna stödja sig på åtminstone en av de nu angivna rättsliga grunderna. För enskilda som inte utför uppgifter av allmänt intresse bör framför allt intresseavvägningsgrunden i artikel 6.1 f aktualiseras vid kamera-bevakning. Av dataskyddsförordningen följer dock att intresse-avvägningen i punkten f inte gäller för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter. Dessa torde i stället kunna tillämpa den rättsliga grunden i artikel 6.1 e om behandling som är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

Av artikel 6.3 i dataskyddsförordningen följer vidare ett krav på att uppgiften av allmänt intresse eller den myndighetsutövning som grundar en rätt att behandla personuppgifter ska fastställas i enlighet med unionsrätten eller den nationella rätten. I förslaget till dataskyddslag finns en bestämmelse som förtydligar att detta krav för svensk del innebär att uppgiften av allmänt intresse ska följa av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning (2 kap. 2 §). Av förslaget framgår vidare att myndighetsutövning som grundar rätt att behandla personuppgifter ska ske enligt lag eller annan författning.

Enligt artikel 35.1 i dataskyddsförordningen ska en konsekvens-bedömning avseende dataskydd göras om en typ av personuppgiftsbehandling, 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. Enligt artikel 35.3 c ska en sådan konsekvensbedömning särskilt krävas vid systematisk övervakning av en allmän plats i stor omfattning. Om en konsekvensbedömning visar att behandlingen skulle leda till en hög risk om inte åtgärder vidtas för att minska risken ska den personuppgiftsansvarige enligt artikel 36.1 dessutom samråda med tillsynsmyndigheten före behandlingen.

I enlighet med artikel 36.5 i dataskyddsförordningen har medlemsstaterna i sin nationella rätt också möjlighet att kräva 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.

Den kamerabevakning som bedrivs av fysiska personer och de flesta företag har sällan en sådan koppling till en uppgift av allmänt intresse som avses i dataskyddsförordningen. Sådan kamerabevakning kommer i stället i normalfallet att bedömas utifrån intresseavvägningsgrunden i artikel 6.1 f. Regeringen instämmer därför i utredningens bedömning att kamerabevakning inom dataskyddsförordningens tillämpningsområde endast delvis kan omfattas av ett tillståndskrav. Inte heller kan ett krav på anmälan av det slag som finns i kameraövervakningslagen behållas generellt.

Kamerabevakning inom det nya dataskyddsdirektivets tillämpningsområde

Det nya dataskyddsdirektivet innehåller inget krav på förhandstillstånd men däremot bestämmelser om skyldigheter att göra konsekvensbedömningar och samråda med tillsynsmyndigheten. Av artikel 27 i direktivet följer exempelvis att 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 medlemsstaterna säkerställa att den personuppgiftsansvarige, eller personuppgiftsbiträdet, före behandlingen utför en bedömning av dess konsekvenser för skyddet av personuppgifter. Enligt artikel 28 i direktivet ska medlemsstaterna vidare föreskriva att den personuppgiftsansvarige i vissa fall ska samråda med tillsynsmyndigheten före en behandling av personuppgifter som kommer ingå i ett nytt register som ska inrättas. Det gäller när en konsekvensbedömning visar att behandlingen skulle leda till en hög risk – om inte den registeransvarige vidtar åtgärder för att minska risken – eller när typen av behandling, särskilt vid användning av ny teknik eller nya rutiner eller förfaranden medför en hög risk för de registrerades rättigheter och friheter.

I förslaget till brottsdatalag finns bestämmelser som genomför dessa artiklar (3 kap. 7 §). Enligt förslaget ska den personuppgiftsansvarige, om en ny typ av behandling, eller betydande förändringar av redan pågående behandling, kan antas medföra särskild risk för intrång i registrerades personliga integritet, innan behandlingen påbörjas eller förändringen genomförs bedöma konsekvenserna för skyddet av personuppgifter. Om konsekvensbedömningen visar att det finns särskild risk för intrång i registrerades personliga integritet eller om typen av behandling innebär särskild risk för intrång, ska den personuppgiftsansvarige vidare samråda med tillsynsmyndigheten i god tid innan behandlingen påbörjas eller betydande förändringar genomförs.

Eftersom det nya dataskyddsdirektivet inte hindrar medlemsstaterna från att föreskriva starkare skyddsåtgärder än de som fastställs i direktivet för skyddet av den registrerades rättigheter och friheter (artikel 1.3) är det möjligt att behålla ett krav på förhandstillstånd för sådan kamerabevakning som omfattas av direktivets tillämpningsområde. För svensk del skulle ett

sådant krav bl.a. omfatta den kamerabevakning som Polismyndigheten, Tullverket och Kustbevakningen bedriver i brottsbekämpande syften.

Kamerabevakning utanför EU-rättens tillämpningsområde

Dataskyddsförordningen och det nya dataskyddsdirektivet omfattar inte personuppgiftsbehandling som utförs som ett led i en verksamhet som inte omfattas av unionsrätten, såsom verksamhet rörande nationell säkerhet eller som omfattas av EU:s gemensamma utrikes- och säkerhetspolitik. Det gäller t.ex. sådan kamerabevakning som bedrivs av Säkerhetspolisen i verksamhet som avser nationell säkerhet eller av myndigheter inom försvaret. Eftersom sådan kamerabevakning inte omfattas av EU-regleringen finns det inget EU-rättsligt hinder mot att ett tillståndskrav ska gälla även fortsättningsvis för sådan kamerabevakning.

6.2 Det nya tillståndskravet

Regeringens förslag: Tillstånd ska krävas till kamerabevakning av en plats dit allmänheten har tillträde, om bevakningen ska bedrivas av en myndighet. Detsamma ska gälla om kamerabevakning av en sådan plats ska bedrivas av någon annan än en myndighet vid utförande av en uppgift av allmänt intresse som följer av lag eller annan författning, kollektivavtal eller beslut som meddelats med stöd av lag eller annan författning.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: En majoritet av remissinstanserna tillstyrker förslaget eller har inga synpunkter på det. *Datainspektionen* anser att det föreligger starka skäl för att kamerabevakning som faller in under det nya dataskyddsdirektivet ska omfattas av ett tillståndskrav. Datainspektionen anser vidare att det är motiverat att behålla tillståndskravet på dataskyddsförordningens område så långt det är möjligt men menar att den föreslagna omfattningen och avgränsningen för andra aktörer än myndigheter blir otydlig. Enligt Datainspektionen är det exempelvis oklart vad som är en uppgift av allmänt intresse. Enligt Datainspektionen uppfyller bestämmelsen inte de krav på tydlighet och förutsebarhet som måste ställas på en tillståndsbestämmelse som omfattas av sanktionsavgifter. Datainspektionen ifrågasätter också om angivande av kollektivavtal generellt som en rättslig grund kan anses följa av dataskyddsförordningen. Det kan enligt Datainspektionen vidare inte uteslutas att myndigheter kan bedriva kamerabevakning med en annan rättslig grund än artikel 6.1 e i dataskyddsförordningen. *Domstolsverket* framhåller att kamerabevakning innebär mycket integritetskänsliga personuppgiftsbehandlingar och menar att ett tillståndskrav inskärper betydelsen av att tillämpliga bestämmelser följs samt ökar efterlevnaden av dem. *Kammarrätten i Stockholm* instämmer i utredningens förslag om att ett tillståndskrav ska fortsätta att gälla i den utsträckning som EU-regleringen lämnar utrymme för det. *Statens skolinspektion* understryker vikten av att såväl offentliga som enskilda huvudmän även fortsättningsvis omfattas av ett tillståndskrav vid kamerabevakning av platser dit allmänheten har tillträde vid skolor. Även *Försvarsmakten* håller i stort

med om det som utredningen föreslår och invänder inte särskilt mot ett fortsatt tillståndskrav som huvudregel. *Polismyndigheten* är däremot kritisk mot förslaget och anför att det saknas vägande skäl för att i nationell rätt ställa upp tillkommande krav på förhandstillstånd från tillsynsmyndigheten inför Polismyndighetens kamerabevakning. Ett fortsatt formellt förfarande med ansökan om tillstånd innebär enligt Polismyndigheten tidsödande administration på ett sätt som inte längre vägs upp av integritetshänsyn mot bakgrund av att den nya EU-regleringen ändå innebär ett stärkt integritetsskydd. Polismyndigheten anser därför att tillståndskravet kan avskaffas för myndighetens kamerabevakning utan att det riskerar att leda till otillbörliga integritetsintrång. *Åklagarmyndigheten*, *Ekobrottsmyndigheten* och *Säkerhet för Näringsliv och Samhälle (SNOS)* delar Polismyndighetens uppfattning och framför i allt väsentligt liknande argument. *Transportstyrelsen* ser positivt på att tillståndskravet inte längre kommer att omfatta privata användares kamerabevakning eftersom det medför fortsatt goda möjligheter att utveckla branschen för kamerautrustade drönare. *Lantmäteriet* anser inte att tillståndskravet bör gälla generellt för myndigheter när privata aktörers kamerabevakning i de flesta fall blir tillståndsfri och åberopar bl.a. vad myndigheten tidigare har gjort gällande om myndigheters behov av att använda drönare (se prop. 2016/17:182 s. 30). *Karlskrona kommun* menar att det kan anses motiverat att behålla en tillståndsplikt i de fall där myndigheternas uppgifter omfattas av en lagstadgad skyldighet och att tillståndskravet också bör gälla privaträttsliga subjekt som har i uppdrag att utföra sådana uppgifter. Karlskrona kommun är dock av uppfattningen att tillståndskravet inte bör gälla för myndigheter när de utför sina frivilliga uppgifter eftersom det i motsvarande situationer inte kommer krävas tillstånd av enskilda aktörer. *Fastighetsägarna* framhåller att den föreslagna formuleringen av tillståndskravet kan väntas orsaka vissa gränsdragningsproblem men menar samtidigt att det lär vara svårt att formulera en mer klargörande princip. *Visita* anser att ett slopat tillståndskrav har potential att förenkla för hotell, restaurang och liknande verksamheter. *Sveriges lantbruksuniversitet* och *Skogsindustrierna* anser att begränsningen av tillståndskravets omfattning underlättar angelägen kamerabevakning inom exempelvis jordbruk och skogsbruk. *Jägarnas riksförbund* ser också positivt på att privatpersoner ska kunna använda viltbevakningskameror utan att omfattas av vare sig ett tillstånds- eller anmälningskrav. *Svenska rovdjursförbundet* motsätter sig dock att åtelkameror ska kunna placeras ut utan föregående tillstånd eller anmälan eftersom det försvårar en effektiv tillsyn och riskerar leda till ökad illegal jakt. *Sveriges advokatsamfund* poängterar att det inte ingår i allemansrätten att utan markägares eller annan rättighetsinnehavares tillstånd bedriva kamerabevakning på annans mark. *SJ AB* motsätter sig den föreslagna utformningen av tillståndskravet eftersom den blir mycket svårtillämplig för järnvägsbranschen. Enligt SJ:s tolkning skulle t.ex. sådan kommersiell tågtrafik som bedrivs av SJ och andra aktörer i stora delar av landet inte omfattas av tillståndskravet medan däremot sådan tågtrafik som har upphandlats enligt lagen (2010:1065) om kollektivtrafik skulle omfattas av nämnda krav. Enligt *Svensk kollektivtrafik* kan den föreslagna utformningen av tillståndskravet och kopplingen till allmänt intresse få orättvisa följder beroende på drifts- och finansieringsform. Svensk

kollektivtrafik invänder dessutom mot att begreppet plats dit allmänheten har tillträde ska anses omfatta platser inom kollektivtrafiken när det krävs en giltig biljett eller färdbevis för att tillträde ska beviljas. *Tjänstemännens centralorganisation (TCO)* anser att all kamerabevakning på arbetsplatser som huvudregel borde vara tillståndspliktig mot bakgrund av de allvarliga integritetskränkningar sådan övervakning kan innebära.

Skälen för regeringens förslag

Tillståndskrav som huvudregel för myndigheter med verksamhet inom dataskyddsförordningens tillämpningsområde

Som konstateras i avsnitt 6.1 utgör regleringen i dataskyddsförordningen ett hinder mot att behålla ett generellt krav på förhandstillstånd för kamerabevakning av platser dit allmänheten har tillträde. Inom dataskyddsförordningens tillämpningsområde kan ett krav på tillstånd endast ställas upp för sådan kamerabevakning som sker vid utförandet av en uppgift av allmänt intresse. Regleringen i dataskyddsförordningen kräver dessutom att uppgiften av allmänt intresse är fastställd i enlighet med nationell rätt.

Det nu sagda innebär att myndigheter med verksamhet inom dataskyddsförordningens tillämpningsområde i och för sig kan omfattas av ett krav på tillstånd för kamerabevakning. Myndigheternas verksamhet består i myndighetsutövning eller andra uppgifter av allmänt intresse.

Det finns flera skäl som talar för att ett tillståndskrav bör gälla generellt för myndigheter som bedriver sådan kamerabevakning som omfattas av dataskyddsförordningen. Ett tillståndskrav har gällt under lång tid för myndigheters kamerabevakning i syfte att garantera ett starkt integritetsskydd och det har inte framkommit att ett tillståndskrav i sig skulle utgöra ett hinder eller försvåra ändamålsenlig kamerabevakning i de aktuella myndigheternas verksamhet. Ett tillståndskrav underlättar också tillsynsarbetet och ger goda förutsättningar för tillsynsmyndigheten att i förväg göra bedömningar av kamerabevakningens tillåtlighet. När ett tillstånd väl har meddelats får den som bedriver kamerabevakningen ett klart besked att rätta sig efter i stället för att riskera invändningar och tillsynsprocesser efter det att kamerabevakningen har kommit igång. Samtidigt som tillståndskravet syftar till att garantera ett starkt integritetsskydd ger det också goda möjligheter att närmare reglera villkoren för när sådana tillstånd ska meddelas, vilket i sin tur kan bidra till att snabbt få till stånd en enhetlig och mer ändamålsenlig rättstillämpning.

Karlskrona kommun förespråkar en ordning där tillståndskravet endast gäller för myndigheter vid utförandet av uppgifter som omfattas av en lagstadgad skyldighet. Som utredningen konstaterar skulle dock en sådan avgränsning innebära nya gränsdragningsproblem, eftersom det i vissa fall kan vara svårt att avgöra vad som är en obligatorisk respektive en frivillig uppgift för en kommun. Det som tidigare har betraktats som ett frivilligt åtagande kan dessutom ändra karaktär över tid. Så har t.ex. flyktingmottagandet gått från att vara en frivillig till en tvingande uppgift för kommunerna. Tillståndskravet för myndigheter bör därför inte innehålla någon begränsning av detta slag.

Många myndigheters användning av kamerautrustade drönare kommer vidare att underlättas av att kamerabevakningslagen får ett snävare tillämpningsområde än kameraövervakningslagen och enbart omfattar sådan användning av kameror som innebär en varaktig eller regelbundet upprepad personbevakning. Därmed kommer användning av drönare vid exempelvis besiktningar, tillsyn och mätningar ofta kunna ske tillståndsfritt, vilket bl.a. underlättar för Lantmäteriet och andra myndigheter som använder drönare för andra syften än personbevakning.

Sammanfattningsvis bör tillståndskravet för kamerabevakning alltså behållas för myndigheter vars verksamhet omfattas av dataskyddsförordningens tillämpningsområde.

Tillståndskravet bör också behållas för vissa privaträttsliga subjekt

Frågan är då om tillståndskravet även bör omfatta viss kamerabevakning som bedrivs av privaträttsliga subjekt inom dataskyddsförordningens tillämpningsområde. Enligt dataskyddsförordningen kan ett sådant tillståndskrav gälla förutsatt att kamerabevakningen sker för att utföra en uppgift av allmänt intresse som är fastställd i enlighet med nationell rätt.

De skäl som anförs ovan för att tillståndskravet ska gälla myndigheters kamerabevakning talar även för att kravet bör gälla när uppgifter av allmänt intresse har anförtrotts privaträttsliga subjekt. Avmonopolisering och konkurrensutsättning av offentlig verksamhet har inneburit att många uppgifter som tidigare utförts av statliga eller kommunala myndigheter i dag sköts av andra. Inom den traditionellt statliga sektorn kan nämnas t.ex. järnvägstransporter. Som exempel på det kommunala området kan nämnas skola och hälso- och sjukvård. Det skulle framstå som inkonsekvent att kräva tillstånd till kamerabevakning för myndigheter men inte när ett privaträttsligt subjekt ska bedriva kamerabevakning vid utförandet av en sådan uppgift av allmänt intresse, särskilt som sådan kamerabevakning kan vara mycket integritetskänslig.

Som konstateras ovan innebär ett fortsatt tillståndskrav också möjligheter att närmare reglera villkoren för när sådana tillstånd ska meddelas, vilket kan bidra till att snabbare få till stånd en enhetlig och ändamålsenlig rättstillämpning på området.

Mot denna bakgrund bör tillståndskravet behållas som huvudregel för kamerabevakning som bedrivs av andra än myndigheter i den utsträckning som dataskyddsförordningen tillåter det (se s. 60–62 för utvecklat resonemang och exempel).

Inget tillståndskrav för merparten av enskilda

Till följd av de anpassningar som nu sker till EU-regleringen kommer ett tillståndskrav inte att kunna gälla för merparten av privata subjekts kamerabevakning. Inte heller kan en reglering som motsvarar dagens reglering om kameraövervakning som är tillåten efter anmälan behållas. Många remissinstanser välkomnar en sådan ordning och förutser att det kommer innebära ökade möjligheter till kamerabevakning än i dag, bl.a. inom skogsbruk, lantbruk och jakt. Också sådan kamerabevakning som religiösa samfund bedriver i anslutning till sina lokaler kommer att kunna ske utan krav på tillstånd.

Mycket talar för att kamerabevakning utanför det tillståndspliktiga området kommer att vara tillåten i högre utsträckning än vad som är fallet i dag. Detta beror framför allt på att dataskyddsförordningen tillåter personuppgiftsbehandling för fler ändamål än vad som följer av den nuvarande kameraövervakningslagen. Det är samtidigt viktigt att framhålla att kamerabevakning utanför det tillståndspliktiga området inte kommer att kunna ske fritt framöver. I normalfallet gäller exempelvis dataskyddsförordningens grundläggande krav på laglig behandling av personuppgifter i artikel 6 och de allmänna principer om bl.a. ändamålsbegränsning och lagringsminimering som ställs upp i artikel 5.1. Som nämns ovan kommer enskilda subjekts kamerabevakning oftast att grunda sig på en intresseavvägning i enlighet med artikel 6.1 f i dataskyddsförordningen. Detta innebär att kamerabevakningen kommer att vara tillåten om den är nödvändig för ändamål som rör den personuppgiftsansvariges eller tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre.

I de fall där tillståndsfri kamerabevakning innebär särskilt höga integritetsrisker ställer dessutom dataskyddsförordningen krav på att den som bedriver kamerabevakningen ska göra en konsekvensbedömning av dataskydd (artikel 35.1) och i vissa fall även samråda med tillsynsmyndigheten (artikel 36.1). Tillsynsmyndigheten ska upprätta och offentliggöra en förteckning över de typer av behandlingsverksamheter som omfattas av kravet på konsekvensbedömning avseende dataskydd (artikel 35.4) och får också ta fram en motsvarande förteckning med behandlingsverksamheter som inte kräver någon sådan konsekvensbedömning (artikel 35.5). Redan av regleringen i dataskydds-förordningen följer emellertid att en konsekvensbedömning krävs vid systematisk övervakning av en allmän plats i stor omfattning (artikel 35.3 c). I enlighet med de riktlinjer som antagits av den s.k. artikel 29-gruppen är kravet på konsekvensbedömning primärt tillämpligt på sådana behandlingssituationer som initierats efter att dataskyddsförordningen börjar tillämpas den 25 maj 2018 och på befintliga behandlingar där riskerna av något skäl har ändrats (Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, WP 248 rev.01).

Även sådan kamerabevakning som inte omfattas av tillståndskravet kommer att omfattas av kamerabevakningslagens krav på upplysning (se avsnitt 7) och tystnadsplikt (se avsnitt 10). Vid överträdelser av upplysningskravet kan lagens bestämmelser om sanktionsavgifter och skadestånd aktualiseras (se avsnitt 11).

Även annan reglering, exempelvis straffbestämmelsen om kränkande fotografering, kan ha betydelse för frågan om kamerabevakning är tillåten eller inte. Som exempelvis *Advokatsamfundet* framhåller kan det också finnas andra typer av begränsningar, t.ex. när det gäller att sätta upp kameror på annans mark utan tillstånd från markägaren.

Tills vidare ett fortsatt tillståndskrav för kamerabevakning inom det nya dataskyddsdirektivets område

Kamerabevakning förekommer i stor utsträckning i verksamheter inom det nya dataskyddsdirektivets tillämpningsområde, inte minst genom Polismyndighetens kamerabevakning i brottsbekämpande syften. Sådan kamerabevakning sker ofta av platser där många människor rör sig och är direkt inriktad på att kontrollera människors förehavanden.

Ordningen med ett tillståndskrav för kamerabevakning i de verksamheter och syften som avses i det nya dataskyddsdirektivet har funnits länge och är avsedd att garantera ett starkt skydd mot bevakning av enskilda och samtidigt ge ändamålsenliga möjligheter till kamerabevakning. Utredningens kartläggning visar dock på en för restriktiv tillämpning av möjligheterna att få tillstånd. Vidare har framkommit att ett tillståndsförfarande kan, som *Polismyndigheten* framhåller, innebära tidsödande administration och minskad flexibilitet i det brottsbekämpande arbetet.

Ett tillståndsförfarande kan som nämns ovan innebära vissa fördelar från verksamhetssynpunkt. När ett tillstånd har meddelats får den som bedriver kamerabevakningen ett klart besked att rätta sig efter i stället för att riskera invändningar och tillsynsprocesser efter det att kamerabevakningen har kommit igång. Att behålla tillståndskravet och samtidigt närmare reglera villkoren för när sådana tillstånd ska meddelas kan dessutom innebära möjligheter att snabbt få till stånd en enhetlig och mer ändamålsenlig rättstillämpning på området.

Det nu redovisade talar i och för sig för att kamerabevakningslagen bör innehålla ett krav på tillstånd också för sådan kamerabevakning som träffas av det nya dataskyddsdirektivet. Regeringen är samtidigt angelägen om att sådan kamerabevakning som Polismyndigheten och vissa andra brottsbekämpande myndigheter bedriver inte försvåras om ett fullgott integritetsskydd kan uppnås på andra sätt. Ett alternativ till tillståndskravet skulle exempelvis kunna vara någon form av anmälningsplikt. Detta skulle minska de administrativa bördor som Polismyndigheten hänvisar till och samtidigt ge tillsynsmyndigheten goda möjligheter att undersöka om kamerorna används i enlighet med gällande regleringar.

Som framgår av avsnitt 3 har riksdagen gett regeringen till känna att polisens tillståndskrav för kameraövervakning ska tas bort och ersättas av en anmälningsplikt senast i samband med att den nya kamerabevakningslagen träder i kraft den 25 maj 2018. Regeringen instämmer i att polisens tillståndskrav bör tas bort och i första hand ersättas av en anmälningsplikt. Frågan behandlas dock inte närmare av utredningen och med hänsyn till frågans komplexitet har det inte varit möjligt att, inom ramen för regeringsformens beredningskrav, hinna ta fram förslag som kan behandlas i detta lagstiftningsärende. Som framgår av avsnitt 5.2.2 har regeringen däremot tillsatt en utredning som ska föreslå förenklingar vid kamerabevakning som sker i brottsbekämpande syfte. Syftet med utredningen är att säkerställa att myndigheternas möjlighet att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda brott och att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, ska vara flexibel och verksamhetsanpassad. Utredningen ska mot denna bakgrund föreslå förenklingar för sådan kamerabevakning som

bl.a. Polismyndigheten men också andra brottsbekämpande myndigheter bedriver, med utgångspunkten att tillståndsplikten ska tas bort och i första hand ersättas med en anmälningsplikt. I denna del ska utredningens förslag redovisas senast den 15 augusti 2018.

Mot denna bakgrund bör kamerabevakningslagen tills vidare innehålla ett tillståndskrav som huvudregel för sådan kamerabevakning som omfattas av det nya dataskyddsdirektivets tillämpningsområde. Enligt regeringens bedömning finns det dock ett tydligt behov av att förbättra möjligheterna att få tillstånd och att införa utvidgade undantag från tillståndskravet (se avsnitt 6.3 och 6.5).

Ett fortsatt tillståndskrav för kamerabevakning i verksamheter utanför EU-rätten

De skäl som anförs för ett fortsatt krav på tillstånd för kamerabevakning som omfattas av dataskyddsförordningens respektive det nya dataskyddsdirektivets tillämpningsområde gör sig i allt väsentligt gällande även för kamerabevakning i sådan verksamhet som faller utanför EU-rättens tillämpningsområde, exempelvis kamerabevakning som bedrivs av Försvarsmakten eller Säkerhetspolisen i verksamhet som rör nationell säkerhet.

Att ett och samma tillståndskrav gäller för sådan kamerabevakning innebär också att eventuell gränsdragningsproblematik i förhållande till dataskyddsförordningens respektive det nya dataskyddsdirektivets tillämpningsområde undviks. Några särskilda invändningar mot att behålla tillståndskravet som huvudregel för kamerabevakning i nu aktuella verksamheter framförs inte heller av remissinstanserna.

Ett tillståndskrav bör därför gälla som huvudregel även för kamerabevakning som bedrivs av en myndighet eller en annan aktör i en verksamhet som faller utanför dataskyddsförordningens och det nya dataskyddsdirektivets tillämpningsområde.

Tillståndskravet ska endast avse platser dit allmänheten har tillträde

Tillståndskravet i den nuvarande kameraövervakningslagen gäller endast för platser dit allmänheten har tillträde. Med sådana platser avses exempelvis gator, torg och parker men också transportmedel som används för allmänna kommunikationer eller evenemang dit vem som helst kan lösa en biljett. Även om *Svensk kollektivtrafik* invänder mot en sådan tolkning av begreppet har det blivit föremål för en förhållandevis omfattande rättspraxis. Vid införandet av kameraövervakningslagen ansågs det inte heller lämpligt att definiera begreppet i lagtexten (se prop. 2012/13:115 s. 34).

Mot denna bakgrund instämmer regeringen i utredningens bedömning att tillståndskravet i kamerabevakningslagen bör avse platser dit allmänheten har tillträde. Att, som *Tjänstemännens centralorganisation (TCO)* förespråkar, låta tillståndskravet gälla för samtliga arbetsplatser, dvs. även arbetsplatser dit allmänheten inte har tillträde, skulle innebära en kraftig utvidgning av det nuvarande tillståndskravets omfattning. Det förefaller dessutom tveksamt om ett sådant krav skulle utgöra en tillåten nationell specificering för personuppgiftsbehandling i anställningsförhållanden enligt artikel 88 i dataskyddsförordningen.

Integritetsskyddet på arbetsplatser dit allmänheten inte har tillträde bör i stället förstärkas på ett annat sätt, se avsnitt 8.

Bestämmelsens närmare utformning

Kravet på tillstånd bör av tydlighetsskäl tas in i en bestämmelse där kravet uttrycks samlat för myndigheterna och övriga aktörer som omfattas av kravet. Utredningen föreslår en bestämmelse om att tillstånd krävs till kamerabevakning av en plats dit allmänheten har tillträde, om bevakningen ska bedrivas av en myndighet. Detsamma ska enligt utredningens förslag gälla om kamerabevakning av en sådan plats ska bedrivas av en annan juridisk person eller en fysisk person vid utförande av en uppgift som följer av lag eller annan författning, kollektivavtal eller beslut som meddelats med stöd av lag eller annan författning och 1) avser brottsbekämpning, lagföring eller straffverkställighet eller upprätthållande av allmän ordning och säkerhet, 2) avser nationell säkerhet, eller 3) annars är av allmänt intresse.

Enligt *Datainspektionen* är det tänkbart att myndigheter skulle kunna bedriva kamerabevakning med stöd av en annan rättslig grund i dataskyddsförordningen än att kamerabevakningen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning. Detta skulle enligt Datainspektionen innebära att en tillståndsansökan inte kan prövas eftersom dataskyddsförordningen inte lämnar utrymme för ett sådant förfarande utanför de nu aktuella rättsliga grunderna. Regeringen har dock svårt att se i vilka fall kamerabevakning skulle vara nödvändig för en myndighet i enlighet med någon av de övriga rättsliga grunderna i dataskyddsförordningen utan att samtidigt vara nödvändig för en uppgift av allmänt intresse. Det finns därför inte skäl att utforma tillståndskravet för myndigheter på något annat sätt än vad utredningen föreslår. Med myndigheter avses i enlighet med regeringsformens terminologi samtliga statliga och kommunala organ, med undantag av riksdagen, kommun- och landstingsfullmäktige. Organ som är organiserade i privaträttsliga former, t.ex. kommunala och statliga bolag, är dock inte myndigheter, även om de utövar offentlig makt.

När det gäller utformningen av tillståndskravet för andra än myndigheter bör i enlighet med utredningens bedömning ett alternativ väljas som är förenligt med regleringen i dataskyddsförordningen, ger ett tillfredsställande integritetsskydd och minimerar eventuella tillämpningsproblem. Ett tillståndskrav som utgår från dataskyddsförordningens begrepp uppgift av allmänt intresse samt knyter an till förordningens krav på att uppgiften ska komma till uttryck i unionsrätten eller den nationella rätten innebär att regleringen fullt ut skulle harmoniera med EU-rätten. Det skulle också bli tydligt att tillståndsprövningen i första hand består av en prövning av om kamerabevakningen är laglig enligt EU-regleringen.

Regeringen har viss förståelse för de synpunkter som vissa remissinstanser framför angående den närmare innebörden av begreppet allmänt intresse. Samtidigt finns det som utredningen anför fördelar med att använda just det begrepp som används i dataskyddsförordningen och vars närmare innebörd väntas bli föremål för både svensk och EU-rättslig praxis. Rent språkligt kan begreppet uppgift av allmänt intresse antas avse

något som är av intresse för eller berör många människor på ett bredare plan, i motsats till ett särintresse eller ett enskilt intresse. Av skäl 45 till dataskyddsförordningen följer att allmänintresset inbegriper hälso- och sjukvårdsändamål, folkhälsa, socialt skydd och förvaltning av hälso- och sjukvårdstjänster. Det kan vidare konstateras att begreppet förekommer i motsvarande bestämmelser i det nuvarande dataskyddsdirektivet (artikel 7 e) och personuppgiftslagen (10 § d) och att ledning därför kan hämtas från hur begreppet tolkats enligt dessa bestämmelser.

En sådan utformning av tillståndskravet som nu diskuteras innebär också att det i första hand träffar den typen av verksamheter som lika gärna hade kunnat bedrivas av statliga myndigheter, landsting eller kommuner. Tillståndskravet skulle exempelvis omfatta kamerabevakning inom hälso- och sjukvård generellt, dvs. oavsett vem som bedriver verksamheten, förutsatt att det rör sig om bevakning av utrymmen som allmänheten har tillträde till. Tillståndskravet skulle också omfatta skolområden dit allmänheten har tillträde, liksom kollektivtrafik, järnvägstrafik och flygtrafik förutsatt att den som bedriver verksamheten kan anses utföra en uppgift av allmänt intresse som är fastställd i gällande rätt.

I syfte att tydliggöra i vilka fall en uppgift anses vara av allmänt intresse i aktuell bemärkelse bör, som utredningen också föreslår, en motsvarande förtydligande bestämmelse som finns i 2 kap. 2 § 1 i förslaget till dataskyddslag användas. Det bör således framgå att uppgiften av allmänt intresse ska följa av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Bestämmelsen i kamerabevakningslagen bör i denna del utformas på samma sätt som bestämmelsen i förslaget till dataskyddslag även om det sällan torde vara aktuellt att åberopa kollektivavtal som en rättslig grund för kamerabevakning vid utförandet av en uppgift av allmänt intresse.

Vissa remissinstanser, däribland *SJ AB* och *Svensk kollektivtrafik*, invänder mot den föreslagna utformningen av bestämmelsen och menar att den är svår att tillämpa och skulle leda till orättvisa följder beroende på drifts- och finansieringsform. När det gäller järnvägstransporter och kollektivtrafik bör bestämmelsen emellertid enligt regeringens bedömning i princip omfatta sådan verksamhet, oavsett vilket typ av subjekt som bedriver den. Detta eftersom uppgiften att bedriva sådan trafik typiskt sett måste anses utgöra ett allmänt intresse som är fastställd på det sätt som anges i bestämmelsen. Kapacitetstilldelningen är exempelvis föremål för en omfattande och hårt reglerad process. Av 6 och 7 kap. järnvägslagen (2004:519) samt 5 kap. järnvägsförordningen (2004:526) följer bl.a. att den som vill ha ett tågläge ansöker om detta hos Trafikverket som, om inte alla ansökningar kan bifallas, fördelar kapaciteten utifrån samhällsekonomisk nytta.

Det kan vidare konstateras att verksamhet i privat och offentlig regi ofta omfattas av en och samma reglering. För hälso- och sjukvårdsverksamhet fastställs exempelvis uppgiften av allmänt intresse i bl.a. hälso- och sjukvårdslagen (2017:30). På motsvarande sätt fastställs skolväsendets uppgifter i skollagen (2010:800).

Mot denna bakgrund kommer alltså kamerabevakning av järnvägstrafik, kollektivtrafik och flygplatser i de allra flesta fall att omfattas av tillståndskravet och behandlas på ett likvärt sätt oavsett drifts- och finansieringsform. Detsamma gäller kamerabevakning i skolor och inom

hälso- och sjukvården. Om det ändå skulle förekomma osäkerhet är det givetvis angeläget att tillsynsmyndigheten kan öka medvetenheten och förståelsen av regleringen. Därtill kommer att tillståndsprövningen, liksom tillsynen, enligt regeringens förslag ska samlas hos en myndighet vilket ger goda förutsättningar för en enhetlig tillämpning. Datainspektionen bör i sin egenskap av tillsynsmyndighet informera om vilka typer av kamerabevakning som omfattas av tillståndskravet. Dessutom bör en personuppgiftsansvarig vid tveksamheter kunna vända sig direkt till Datainspektionen för vägledning i frågan. I sammanhanget bör också nämnas att den utredning om förenklade möjligheter till kameraövervakning som regeringen har tillsatt ska analysera om ett utökat undantag från tillståndsplikten för kameraövervakning av allmänna transportmedel och stationer bör införas (dir. 2017:124).

Med anledning av vad *Datainspektionen* anför om tillståndskravets förhållande till sanktionsavgifter bör understrykas att sanktionsavgifter inte bör komma i fråga som en första åtgärd i tveksamma fall. I stället bör den som i sådana fall gjort en felaktig tolkning av omfattningen av tillståndskravet ges möjlighet att rätta sig. Det kan exempelvis ske genom olika typer av förelägganden eller varningar.

De privata subjekt som omfattas av tillståndskravet kommer huvudsakligen att bedriva kamerabevakning i verksamheter som omfattas av dataskyddsförordningens tillämpningsområde. Det kan dock inte uteslutas att privata subjekt skulle kunna anförtros uppgifter också inom det nya dataskyddsdirektivets tillämpningsområde eller utanför EU-rättens tillämpningsområde, exempelvis uppgifter som avser nationell säkerhet på försvarsområdet. I enlighet med utredningens förslag bör dataskyddsförordningens krav på att uppgiften ska ha stöd i gällande rätt gälla också i sådana fall. Uppgifter som faller inom det nya dataskyddsdirektivets tillämpningsområde är emellertid alltid av allmänt intresse. Detsamma gäller uppgifter som privaträttsliga subjekt skulle kunna anförtros inom området för nationell säkerhet. Enligt regeringens bedömning finns det därför inte skäl att, som utredningen föreslår, särskilt peka ut dessa uppgifter i bestämmelsen. Bestämmelsen bör alltså formuleras något annorlunda än utredningens förslag.

Kamerabevakningslagen bör sammanfattningsvis innehålla en bestämmelse om att tillstånd krävs till kamerabevakning av en plats dit allmänheten har tillträde, om bevakningen ska bedrivas av en myndighet. Detsamma gäller om kamerabevakning av en sådan plats ska bedrivas av någon annan än en myndighet vid utförande av en uppgift av allmänt intresse som följer av lag eller annan författning, kollektivavtal eller beslut som meddelats med stöd av lag eller annan författning.

6.3 Möjligheterna att få tillstånd ska förbättras

Regeringens förslag: Tillstånd till kamerabevakning ska ges om intresset av sådan bevakning väger tyngre än den enskildes intresse av att inte bli bevakad.

Vid bedömningen av intresset av kamerabevakning ska det särskilt beaktas om bevakningen behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott på en brottsutsatt plats eller på en annan plats där det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet eller på egendom,

2. förebygga, förhindra eller upptäcka störningar av allmän ordning och säkerhet eller begränsa verkningarna av sådana störningar,

3. utöva kontrollverksamhet,

4. förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor, eller

5. tillgodose andra därmed jämförliga ändamål.

Vid bedömningen av den enskildes intresse av att inte bli bevakad ska det särskilt beaktas

1. hur bevakningen ska utföras,

2. om teknik som främjar skyddet av den enskildes personliga integritet ska användas, och

3. vilket område som ska bevakas.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: En majoritet av remissinstanserna är positiva till förslaget eller har inga synpunkter på det. Flera remissinstanser, bl.a. *Karlskrona kommun*, *Malmö kommun* och *Sveriges Kommuner och Landsting*, är särskilt positiva till att det ska bli enklare att få tillstånd till kamerabevakning i och med att fler ändamål ska beaktas särskilt vid bedömningen av intresset för kamerabevakning. Enligt *Datainspektionen* bör det framgå direkt av ordalydelsen av bestämmelsen att det ska ske en prövning av behandlingens laglighet i förhållande till dataskyddsförordningen eller brottsdatalagen. Datainspektionen efterfrågar också tydligare vägledning av hur begreppet brottsutsatt plats skiljer sig från det i praxis etablerade begreppet särskilt brottsutsatt plats. Datainspektionen delar utredningens uppfattning om att generella hotbilder ska vägas in vid intresseavvägningen men menar samtidigt att det måste röra sig om en utifrån faktiska omständigheter identifierad och konkret hotbild som måste kunna styrkas för att motivera ett tillstånd. *Domstolsverket* framhåller att den föreslagna bestämmelsen är snarlik vad som i brottsdatalagen utgör rättslig grund för personuppgiftsbehandling och att förslaget av den anledningen kan behöva förtydligas. *Polismyndigheten* anser att det är olyckligt att bestämmelsen utformas på ett sätt som överlåter till rättstillämpningen att avgöra vad som är tillåten kamerabevakning. Vidare menar Polismyndigheten att utredningens synsätt att kamerabevakning ska ses som ett komplement till andra åtgärder och inte som ett naturligt hjälpmedel är föråldrat. Enligt Polismyndigheten bör ett tillstånd till kamerabevakning för myndigheten i regel innefatta tillstånd till upptagning och inspelning av ljud, t.ex. för att med teknikens hjälp kunna detektera ljud från skjutvapen. *Ekobrottsmyndigheten* anser att formuleringen i den föreslagna bestämmelsen om att utreda eller lagföra brott är otydlig och kan uppfattas som att den avser utredning och lagföring av brott i förundersökning, vilket inte är avsikten. Enligt *Tullverket* riskerar formuleringen av bestämmelsen att försämra möjligheterna att få tillstånd till kamerabevakning på platser som inte träffas av begreppen brottsutsatt plats eller angrepp på någons liv, hälsa eller trygghet eller på egendom. Det är enligt Tullverket t.ex.

angeläget att myndigheten har möjlighet att använda kamerabevakning vid hamnar och flygplatser i syfte att kunna förebygga, förhindra eller upptäcka smugglingsbrott. Några remissinstanser, däribland *Länsstyrelsen i Dalarnas län*, anser att det vid intresseavvägningen bör tas särskild hänsyn till om avsikten med kamerabevakningen inte är att övervaka människor. Länsstyrelsen anser vidare att innebörden av begreppet andra därmed jämförliga ändamål bör förtydligas med hänsyn till behovet av bevakning inom myndigheters uppdrag avseende bl.a. miljö, natur, inventering av djur eller annan viltvård. Enligt länsstyrelsen bör det även förtydligas på vilket sätt ökade möjligheter till kamerabevakning kan ges inom dessa områden. *Luleå tekniska universitet* tolkar förslaget som att det skulle vara svårare att få tillstånd för kamerabevakning avseende forskningsområden som inte omfattas av de särskilt angivna ändamålen och ifrågasätter om en sådan ordning är avsedd.

Skälen för regeringens förslag och bedömning

Möjligheterna att få tillstånd till kamerabevakning bör förbättras

Som framgår av avsnitt 5.2.2 delar regeringen utredningens bedömning att förutsättningarna att få tillstånd enligt kameraövervakningslagen är för snävt utformade, både vad gäller övervakning i brottsbekämpande syften och för andra ändamål. Sådan kamerabevakning som även fortsättningsvis omfattas av ett tillståndskrav, dvs. kamerabevakning som bedrivs av myndigheter och andra subjekt som utför uppgifter av allmänt intresse, är dessutom många gånger den mest angelägna i samhället. Möjligheterna att få tillstånd för kamerabevakning bör därför förbättras generellt. Det är särskilt betydelsefullt att tillstånd kan beviljas i tillräcklig utsträckning för sådan kamerabevakning som används i brottsbekämpande syften och för att skapa tryggare offentliga miljöer.

Det är också angeläget att möjligheterna att använda kamerabevakning i Sverige inte är sämre än vad som gäller generellt inom EU. För det första är det tveksamt om en sådan ordning är tillåten inom dataskyddsförordningens tillämpningsområde och för det andra är det angeläget att svenska brottsbekämpande myndigheter inte har sämre förutsättningar att använda tekniska hjälpmedel vid brottsbekämpning och gränsöverskridande samarbete än motsvarande myndigheter i andra EU-länder.

En intresseavvägning som avgör om kamerabevakningen är laglig

Den nya kamerabevakningslagen bör liksom kameraövervakningslagen innehålla bestämmelser om vilka särskilda hänsyn som ska tas vid tillståndsprövningen. Detta är en nödvändig förutsättning för en enhetlig och ändamålsenlig rättstillämpning på området.

Inom dataskyddsförordningens tillämpningsområde måste denna typ av bestämmelser betraktas som en sådan tillåten nationell specificering som anpassar tillämpningen av förordningens bestämmelser i syfte att säkerställa en laglig och rättvis behandling av personuppgifter (artikel 6.2 i dataskyddsförordningen). Vad som är en laglig och rättvis behandling av personuppgifter avgörs dock i slutändan genom en tillämpning av regleringen i dataskyddsförordningen. Detta innebär, i linje med det som

Datainspektionen anför, att tillståndsprövningen inom dataskyddsförordningens tillämpningsområde i första hand ska ta sikte på en prövning av om kamerabevakningen är förenlig med regleringen i förordningen. På motsvarande sätt måste tillståndsprövningen inom det nya dataskyddsdirektivets tillämpningsområde primärt utgå från en bedömning av om kamerabevakningen är förenlig med regleringen i brottsdatalagen eller annan personuppgiftsreglering som genomför dataskyddsdirektivet, t.ex. polisdatalagen. Regeringen delar inte Datainspektionens uppfattning att bestämmelsen behöver formuleras annorlunda för att tydliggöra detta.

För att prövningen ska ske på ett förutsebart sätt med säkerställande av att både behovet av kamerabevakning och rätten till skydd för den personliga integriteten tillgodoses bör vid prövningen i enlighet med utredningens förslag även fortsättningsvis göras en intresseavvägning.

Vid intresseavvägningen ska liksom tidigare intresset av kamerabevakningen vägas mot den enskildes intresse av att inte bli bevakad. Tillstånd ska ges i de fall där intresset för kamerabevakningen väger tyngre än den enskildes intresse av att inte bli bevakad. En sådan ordning är förenlig med EU-regleringen. För att bevakningsintresset ska kunna väga tyngre än den enskildes intresse av att inte bli bevakad är en första förutsättning att det finns en rättslig grund för kamerabevakningen i annan tillämplig dataskyddsreglering.

När det gäller intresset av kamerabevakning har den svenska regleringen under längre tid präglats av synsättet att kamerabevakning endast bör utgöra ett komplement till andra åtgärder i samma syfte, särskilt brottsförebyggande åtgärder (se bl.a. prop. 2012/13:115 s. 47). Det har exempelvis inte ansetts förenligt med kameraövervakningslagens syfte att godta en övervakning vars ändamål lämpligen kan tillgodoses på något annat mindre integritetskränkande sätt, t.ex. genom bättre belysning och anpassning av vegetation för att försvåra brottslighet. Utredningen gör bedömningen att denna princip bör gälla även i fortsättningen. Regeringen anser dock i likhet med *Polismyndigheten* att det finns anledning att anlägga ett delvis annorlunda synsätt på användning av kameratekniken än det som gällt tidigare. Som Polismyndigheten anför bör kameratekniken numera ses som ett naturligt hjälpmedel i det brottsbekämpande arbetet och inte som en åtgärd som kan tas till först om andra tänkbara åtgärder inte gett resultat. Detta synsätt är enligt regeringens uppfattning också förenligt med EU-regleringen. Där uppställs ett krav på att en behandling av personuppgifter ska vara nödvändig för att den ska få ske. Det unionsrättsliga begreppet nödvändig anses dock inte ha den strikta innebörden att något absolut behövs. Det har exempelvis ansetts att effektivitetsvinster vid behandling av personuppgifter kan innebära att behandlingen ska anses nödvändig och därmed tillåten (SOU 2017:39 s. 105–106).

Regeringen delar däremot inte Polismyndighetens uppfattning att det genom bestämmelsens utformning överlåts till rättstillämpningen att avgöra vad som är tillåten kamerabevakning på ett sätt som riskerar att gå ut över de brottsbekämpande myndigheternas verksamhetsbehov. En av fördelarna med tillståndsförfarandet är att specifika kriterier kan ställas upp i den nationella rätten som ger god ledning till rättstillämpningen, särskilt när det är fråga om angelägen kamerabevakning för

brottsbekämpande ändamål. Detta kan i sin tur bidra till en tillämpning som både tillgodoser de brottsbekämpande myndigheternas verksamhetsbehov och är korrekt i förhållande till EU-regleringen. Som ett led i denna strävan bör de omständigheter som ska beaktas särskilt vid tillståndsprövningen vara fler till antalet och anges mer utförligt än i kameraövervakningslagen.

Brottsutsatta platser och andra platser med förhöjd hotbild

I kameraövervakningslagen anges att det vid tillståndsprövningen särskilt ska beaktas om kameraövervakning behövs för att förebygga, avslöja eller utreda brott. Enligt praxis krävs att en plats är särskilt brottsutsatt för att intresset av brottsbekämpning ska beaktas särskilt vid tillståndsprövningen. Som utredningen konstaterar är det angeläget att kamerabevakningslagen på ett tydligare sätt än i dag tar hänsyn till såväl intresset av att förebygga brott som intresset att utreda och lagföra framtida brott. Att brott kan utredas och lagföras är av avgörande betydelse för allmänhetens förtroende för straffsystemet vilket i sin tur kan få en generell brottsavhållande verkan. Det bör därför som utredningen föreslår räcka att en plats kan betraktas som brottsutsatt för att detta förhållande ska beaktas särskilt vid tillståndsprövningen.

Vissa remissinstanser, bl.a. *Datainspektionen*, efterfrågar en tydligare vägledning om hur begreppet brottsutsatt plats skiljer sig från det i dag etablerade begreppet särskilt brottsutsatt plats. Det kan först konstateras att en brottsutsatt plats inte är varje plats där det någon gång har inträffat enstaka brott. Däremot bör det inte krävas att brottsligheten är ovanligt hög på platsen för att den ska anses vara brottsutsatt eller att det kan presenteras statistik över brottsligheten på den aktuella platsen i förhållande till andra jämförbara platser. Det som bör kunna visas är i stället att det finns problem med brottslighet där bevakningen ska ske. Det bör samtidigt inte krävas utredning om att brottsligheten är påtagligt hög precis där bevakningen ska ske, dvs. inom de aktuella kamerornas tänkta upptagningsområde. Ett torg, en gågata eller ett stationsområde bör exempelvis kunna betraktas som en brottsutsatt plats i sig, även om ansökan om kamerabevakning bara skulle avse en mindre del av torget, gågatan eller stationsområdet. På motsvarande sett kan kamerabevakning av en viss plats inom ett bostadsområde motiveras av att området i stort kan anses vara brottsutsatt. Om inte särskilda integritetsaspekter gör sig gällande bör tillsynsmyndigheten kunna utgå från sökandens bedömning av var kamerorna ska placeras och hur de ska riktas inom ett brottsutsatt område.

Vissa typer av platser bör vidare på grund av platsens karaktär i princip kunna förutsättas vara brottsutsatta utan att det behöver bevisas i det enskilda fallet. Det kan exempelvis handla om vissa knutpunkter för allmänna kommunikationer eller om gränsövergångar där det behövs insatser mot smugglingsbrott. Detta innebär, tillsammans med den särskilda bestämmelse om kamerabevakning vid kontrollverksamhet som föreslås nedan, att Tullverkets förutsättningar att bedriva kamerabevakning inom myndighetens olika verksamhetsgrenar kommer att förbättras.

För att kamerabevakning i brottsbekämpande syften ska vara verkningsfull och materialet kunna användas i utredningar och vid lagföring krävs regelmässigt en rätt att spela in bildmaterial. Det krav som tidigare gällt enligt praxis att en plats i princip måste kunna visas vara särskilt brottsutsatt för att bildinspelning ska vara tillåten bör därför inte längre gälla.

Inspelning eller avlyssning av ljud har dock sedan länge betraktats som särskilt integritetskänsligt och bör även framöver bli föremål för en noggrann prövning i det enskilda fallet. Om integritetsintrånget kan minimeras på det sätt som *Polismyndigheten* beskriver, dvs. att tekniken endast reagerar på specifika ljud som t.ex. skottlossning, bör det dock normalt kunna godtas att ljudupptagning sker, under förutsättning att behovet finns. I detta sammanhang kan också nämnas att Utredningen om ordning och säkerhet i domstol (Ju 2015:15) föreslår att det ska bli tillåtet att göra en bildupptagning i eller bildöverföring från rättssalar i samband med utlösandet av överfallslarm (SOU 2017:46 s. 169–171). Intresset av att samtidigt kunna ta upp och överföra ljud vid en sådan allvarlig händelse måste anses väga så pass tungt att ett tillstånd till kamerabevakning i sådana och jämförbara fall även bör innefatta en rätt att ta upp och spela in ljud.

Med anledning av *Ekobrottsmyndighetens* synpunkter angående begreppen utreda eller lagföra brott, bör framhållas att dessa inte tar sikte på utredning eller lagföring av redan begångna brott inom ramen för en pågående förundersökning. Begreppen syftar i stället precis som begreppet utreda brott i den nuvarande kameraövervakningslagen på brott som, vid tillståndsprövningen, ännu inte har begåtts. Enligt regeringens bedömning behöver detta inte förtydligas ytterligare i lagtexten.

Ibland kan det vara svårt att slå fast att en plats är brottsutsatt samtidigt som det på objektiva grunder kan konstateras att det finns ett påtagligt behov av kamerabevakning på platsen i trygghetsskapande syfte. Det gäller i första hand platser som inte kan betecknas som brottsutsatta men där det av något skäl ändå finns en särskild risk för angrepp mot människor eller egendom jämfört med andra platser i samhället. Det kan i och för sig röra sig om platser där olika typer av brott har begåtts men också om platser där det av andra skäl kan konstateras en förhöjd hotbild mot människor som vistas på platsen eller mot egendom som finns där. Som exempel kan nämnas asylboenden eller vissa myndigheters entréer, lokaler och fordon. Ett annat exempel är vissa offentliga platser där riskerna för terrorattentat eller andra typer av angrepp mot människor eller egendom av någon anledning är särskilt stora. Utredningens kartläggning visar att det kan vara mycket svårt att få tillstånd till kamerabevakning med åberopande av förhöjda hotbilder av det aktuella slaget, vilket inte är en godtagbar ordning. Utredningen föreslår därför att det vid bedömningen av intresset av kamerabevakning också särskilt ska beaktas om bevakningen behövs för att motverka brottslighet på en plats där det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet eller på egendom.

Till skillnad från *Datainspektionen* anser inte regeringen att det måste röra sig en utifrån faktiska omständigheter identifierad och konkret hotbild mot den aktuella platsen eller de människor som rör sig där för att denna omständighet ska beaktas särskilt. Det kan också vara fråga om generella

hotbilder mot en viss typ av plats, dvs. utan att konkreta hot har riktats mot just den specifika platsen. Hotfull aktivitet riktad mot flera olika asylboenden skulle t.ex. kunna innebära att det anses föreligga en förhöjd hotbild mot sådana boenden i landet generellt som motiverar tillstånd till kamerabevakning. Motsvarande kan t.ex. gälla för entréer till polisstationer eller uppställningsplatser för vissa myndigheters fordon, om det har förekommit angrepp mot sådana platser eller om det av annan särskild anledning kan anses föreligga en förhöjd hotbild mot sådana platser. Detsamma gäller utryckningsfordon med tillhörande personal som riskerar att utsättas för angrepp i samband med insatser i brottsutsatta områden. Enligt regeringens mening bör vidare Polismyndighetens och andra brottsbekämpande myndigheters bedömningar om tillfälliga eller mer bestående förhöjda hotbilder i regel utgöra tillräckligt underlag för att konstatera att det föreligger en sådan risk för angrepp som ska beaktas särskilt vid bedömningen av intresset av kamerabevakning.

Sammanfattningsvis bör vid bedömningen av intresset för kamerabevakning särskilt beaktas om bevakningen behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott på en brottsutsatt plats eller på en annan plats där det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet eller på egendom.

Allmän ordning och säkerhet

Kamerabevakning i syfte att förebygga, förhindra eller upptäcka störningar av allmän ordning och säkerhet eller att begränsa verkningarna av sådana störningar kan utgöra ett berättigat intresse inte endast för Polismyndigheten och andra brottsbekämpande myndigheter utan också för andra som omfattas av kamerabevakningslagens tillståndskrav, t.ex. kommuner eller aktörer som bedriver kollektivtrafik. I kameraövervakningslagen anges inte att detta intresse ska beaktas särskilt vid tillståndsprövningen, vilket kan vara en anledning till att kommuner enligt rättspraxis har svårt att få tillstånd till kamerabevakning av offentliga platser.

Även om uppgiften att bekämpa och lagföra brott i första hand är en fråga för brottsbekämpande myndigheter som Polismyndigheten finns numera en uttalad ambition att stärka samverkan mellan rättsväsendets myndigheter och andra aktörer såsom kommuner, landsting och andra i det civila samhället vad gäller bl.a. brottsförebyggande och trygghetsskapande arbete. Vidare har kommuner ett eget ansvar för allmän ordning och säkerhet inom kommunen. Mot denna bakgrund bör exempelvis kommuner ha betydligt större möjligheter än i dag att bedriva kamerabevakning på platser där det regelmässigt förekommer brottslighet och andra ordningsstörningar.

Vid bedömningen av intresset för kamerabevakning bör därför särskilt beaktas om kamerabevakningen behövs för att förebygga, förhindra eller upptäcka störningar av allmän ordning och säkerhet eller att begränsa verkningarna av sådana störningar.

Kontrollverksamhet

Kamerabevakning kan även vara ett viktigt verktyg vid olika typer av kontrollverksamhet som framför allt bedrivs av myndigheter, exempelvis vid gränskontroll och tullkontroll samt vid kontroll av vattenskyddsområden och miljöfarlig verksamhet. Kontrollverksamhet anges dock inte som ett intresse som särskilt ska beaktas vid tillståndsprövningen enligt kameraövervakningslagen. Regeringen delar utredningens bedömning att detta intresse bör anges i den nya lagen för att förbättra möjligheterna att få tillstånd till kamerabevakning i sådan verksamhet. Detta innebär bl.a. att Tullverkets möjlighet att använda kamerabevakning i sin verksamhet vid exempelvis flygplatser och hamnar kommer att förbättras.

Olyckor

Av den nuvarande kameraövervakningslagen följer att det vid bedömningen av övervakningsintresset vid tillståndsprövningen särskilt ska beaktas om övervakningen behövs för att förhindra olyckor. I takt med teknikutvecklingen har möjligheterna att använda kameror både före och efter olyckor och i samband med olika typer av räddningsinsatser ökat, inte minst genom användningen av drönare.

Eftersom kamerabevakningslagens tillämpningsområde föreslås bli snävare jämfört med den nuvarande kameraövervakningslagen är det troligt att viss användning av kamerateknik i samband med olyckor inte längre kommer att omfattas av lagens tillämpningsområde. Detta eftersom kameraanvändningen inte innebär en varaktig eller regelbundet upprepad personbevakning. Det kommer dock att finnas fall där kamerabevakningslagen är tillämplig och tillståndskravet således gäller. Regeringen anser, i likhet med utredningen, att det i dessa fall är angeläget att den nya lagen säkerställer möjligheterna att använda kamerabevakning i samtliga skeden av ett olycksförlopp.

Mot denna bakgrund bör vid bedömningen av intresset av kamerabevakning särskilt beaktas om kamerabevakningen behövs för att förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor.

Kamerabevakning för andra ändamål

I kamerabevakningslagen bör, liksom i den nuvarande kameraövervakningslagen, anges att det vid en bedömning av intresset för kamerabevakning också särskilt ska beaktas om kamerabevakningen behövs för att tillgodose ändamål som är jämförliga med de som anges i lagen. Exempel på sådana ändamål är myndigheters kamerabevakning i samband med övningar och testverksamhet som anknyter till de ändamål som anges särskilt i lagen. Andra exempel är kamerabevakning för utförande av en uppgift som avser Sveriges säkerhet och som inte omfattas av de tidigare punkterna och kamerabevakning i samband med forskning som avser hur olyckor kan undvikas, t.ex. i trafiken.

Att vissa i lagen angivna ändamål och andra jämförliga ändamål särskilt ska beaktas innebär att kamerabevakning för sådana ändamål kan motivera större integritetsintrång än när bevakning sker för andra ändamål. Det kan dock konstateras att det inte på förhand är möjligt att närmare beskriva alla

ändamål som kan vara berättigade vid kamerabevakning, bland annat eftersom teknikutvecklingen medför att kamerateknikens ständigt får nya användningsområden. Tillstånd till kamerabevakning bör därför, liksom enligt gällande rätt, kunna ges även för ändamål som inte är jämförliga med de som anges i lagen, så länge de kan anses berättigade och intresset av bevakningen väger tyngre än integritetsintresset i det enskilda fallet. Ett sådant exempel kan vara kamerabevakning för inventering av djur eller annan viltvård. I sådana fall kan det dock behöva göras mer ingående överväganden av behovet av kamerabevakning samt av integritetsriskerna och hur dessa kan minskas.

Detta innebär bland annat att även behoven av att använda kamerabevakning vid sådan forskning som *Luleå tekniska universitet* uppmärksammar kan tillgodoses. Som bl.a. *Länsstyrelsen i Dalarna* anför bör det vid intresseavvägningen generellt också tas hänsyn till om syftet med kamerabevakningen är ett annat än att bevaka människor. Det snävare tillämpningsområdet för den nya lagen innebär samtidigt att användning av kamerateknik i andra syften än att bevaka människor ofta kommer att falla utanför kamerabevakningslagens tillämpningsområde.

Enskildas intresse av att inte bli kamerabevakade

Vid intresseavvägningen bör precis som i dag intresset av kamerabevakningen vägas mot den enskildes intresse av att inte bli bevakad. En sådan bestämmelse är förenlig med EU-regleringen och innebär ett fortsatt starkt skydd för den personliga integriteten.

Vid bedömningen av den enskildes intresse av att inte bli kamerabevakad bör liksom enligt kameraövervakningslagen särskilt beaktas hur bevakningen ska utföras, om teknik som främjar skyddet av den enskildes personliga integritet ska användas och vilket område som ska bevakas. Den utvärdering av kameraövervakningslagen som utredningen genomfört visar att integritetsvänlig teknik blivit en allt viktigare faktor vid tillståndsprövningen, vilket inneburit att fler tillstånd har kunnat meddelas än tidigare. Det finns anledning att anta att utvecklingen kommer fortsätta i denna riktning, särskilt som bestämmelser om inbyggt dataskydd och dataskydd som standard har införts i den nya EU-regleringen (artikel 25 i dataskyddsförordningen och artikel 20 i det nya dataskyddsdirektivet).

I detta sammanhang kan även erinras om att integritetsintresset normalt anses vara mindre starkt i fall där de enskilda som kan komma att bli föremål för kamerabevakning samtidigt är de som riskerar att drabbas av sådan brottslighet som bevakningen syftar till att motverka (se t.ex. RÅ 2001 ref. 39).

6.4 Tillståndsförfarandet

Regeringens förslag: En ansökan om tillstånd till kamerabevakning ska göras skriftligen hos tillsynsmyndigheten och innehålla

1. uppgift om den som ska bedriva bevakningen och i förekommande fall den som ska ha hand om bevakningen för tillståndshavarens räkning,

2. uppgift om bevakningens ändamål,

3. en beskrivning av bevakningen, särskilt den utrustning som ska användas, var den ska placeras, det område eller typ av område som ska bevakas och de tider då bevakning ska ske.

4. en bedömning av behovet av bevakningen och bevakningens proportionalitet i förhållande till ändamålet,

5. en bedömning av riskerna för intrång i den personliga integriteten, en beskrivning av de åtgärder som planeras för att hantera riskerna, och

6. uppgift om de omständigheter i övrigt som är av betydelse för prövningen av ärendet.

Om sökanden inte är en myndighet ska ansökan också innehålla uppgift om den lag eller annan författning, kollektivavtal eller beslut som utgör den rättsliga grunden för kamerabevakningen. Om bevakningen avser en arbetsplats ska ett yttrande från ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på arbetsplatsen lämnas in tillsammans med ansökan.

Den kommun där kamerabevakningen ska ske ska få tillfälle att yttra sig före ett beslut om tillstånd, om det av särskild anledning behövs ett yttrande.

Ett beslut om tillstånd ska förenas med villkor om hur bevakningen får anordnas. Villkoren ska avse

1. bevakningens ändamål,

2. den utrustning som får användas och var utrustningen får placeras,

3. det område eller typ av område som får bevakas och de tider då bevakning får ske, samt

4. upplysning om bevakningen, bevarande eller annan behandling av bilder och ljud och andra förhållanden som har betydelse för att skydda enskildas personliga integritet, om sådana villkor behövs för tillståndet.

Ett tillstånd ska kunna meddelas för en begränsad tid. Om förutsättningarna för ett tillstånd ändras, ska nya villkor få beslutas eller, om förutsättningarna för tillstånd inte längre är uppfyllda, tillståndet återkallas.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen lämnar inget förslag om att ansökan i vissa fall ska innehålla uppgift om den lag eller annan författning, kollektivavtal eller beslut som utgör den rättsliga grunden för kamerabevakningen. Enligt utredningens förslag ska vidare den kommun där kamerabevakningen ska ske få tillfälle att yttra sig före ett beslut om tillstånd om det behövs.

Remissinstanserna: *Datainspektionen* anser att en ansökan om tillstånd bör innehålla information om den lag, författning eller dylikt som utgör den rättsliga grunden för kamerabevakningen och att inspektionen bör ges ett bemyndigande att kunna meddela de närmare föreskrifter som behövs om vad en ansökan ska innehålla. Datainspektionen anser vidare att tillståndshavare bör vara skyldiga att anmäla ändrade förhållanden till tillståndsmyndigheten. *Polismyndigheten* anser att de krav som enligt förslaget ställs på en ansökan utgör en stor administrativ börda som är direkt hämmande för brottsbekämpningen. Enligt Polismyndigheten riskerar de fall där kommunen ska yttra sig att leda till tidsutdräkter och det kan dessutom ifrågasättas vilka kommuner som ska tillfrågas när kamerabevakning kan bedrivas över kommungränser, via exempelvis

fordon eller drönare. Enligt *Länsstyrelsen i Dalarna* kan kravet på att tillstånd ska innehålla villkor avseende den utrustning som får användas och var utrustningen får placeras innebära att tillståndshavaren måste ansöka om ändring av tillståndet så snart kamerautrustningen byts ut eller flyttas. *Länsstyrelsen Västra Götalands län* och *Länsstyrelsen i Östergötlands län* anser att det bör förtydligas vad ett yttrande från berörd kommun ska innehålla så att särskilda kommunala aspekter och lokala synpunkter förs fram. *Malmö kommun* anser att tillståndsgivning för kamerabevakning borde hanteras av kommunerna eftersom kommunerna har god lokalkännedom och en närmare kontakt med medborgarna. *Tjänstemännens centralorganisation (TCO)* tillstyrker förslaget men efterlyser vissa förtydliganden av vad som avses med begreppet företräder arbetstagare på arbetsplatsen och vad som gäller om det t.ex. finns flera sådana organisationer.

Skälen för regeringens förslag

Innehållet i en ansökan

En ansökan om kameraövervakning ska enligt kameraövervakningslagen ske skriftligen till länsstyrelsen i det län där övervakningen ska ske (16 §) och innehålla uppgift om och beskrivning av 1) den som ska bedriva kameraövervakningen och i förekommande fall den som ska ha hand om övervakningen för tillståndshavarens räkning, 2) ändamålen med kameraövervakningen, 3) den utrustning som ska användas, 4) den plats där utrustningen ska placeras och det område som kan övervakas, och 5) de omständigheter i övrigt som är av betydelse för prövningen av ärendet (17 §). Om övervakningen avser en arbetsplats, ska ett yttrande från skyddsombudet, skyddskommittén eller en organisation som företräder de anställda på arbetsplatsen också lämnas in tillsammans med ansökan.

Det har inte framkommit att det finns några problem vid tillämpningen av den nuvarande ordningen varför en ansökan om kamerabevakning enligt den nya lagen bör innehålla motsvarande uppgifter. För att underlätta tillståndsförfarandet vid kamerabevakning från rörliga objekt som exempelvis fordon eller drönare bör det emellertid framgå av lagen att en ansökan kan innehålla en beskrivning av den typ av område som ska bevakas i stället för ett särskilt utpekat område.

Med anledning av *Tjänstemännens centralorganisations (TCO)* synpunkter kan konstateras att uttrycket företräder arbetstagare på arbetsplatsen används i kameraövervakningslagen och att någon ändring av uttryckets innebörd inte är avsedd. Om det finns flera arbetstagargrupper på arbetsplatsen kan det behövas yttranden från företrädare för var och en av dem. Om företrädare av det aktuella slaget inte finns bortfaller däremot kravet.

I dataskyddsförordningen och det nya dataskyddsdirektivet anges hur den personuppgiftsansvarige ska göra en konsekvensbedömning avseende dataskydd i de fall där en sådan behövs. En sådan konsekvensbedömning ska enligt dataskyddsförordningen bl.a. innehålla en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftet (artikel 35.7). Den ska också innehålla en bedömning av riskerna för de registrerades rättigheter och friheter samt de åtgärder som planeras för att hantera riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner

för att säkerställa skyddet av personuppgifter och för att visa att förordningen efterlevs. Enligt det nya dataskyddsdirektivet ska en konsekvensbedömning utöver en allmän beskrivning av den planerade behandlingen innehålla en bedömning av riskerna för de registrerades rättigheter och friheter samt de åtgärder som planeras för att hantera riskerna för att säkerställa skyddet för personuppgifter och för att visa att direktivet efterlevs (artikel 27.2).

Det svenska tillståndskravet för viss kamerabevakning utgör en precisering av den skyldighet att göra en konsekvensbedömning som i många fall hade gällt ändå enligt EU-regleringen. De krav på innehållet i en ansökan om tillstånd som ställs upp i kamerabevakningslagen bör därför utformas i nära anslutning till dataskyddsförordningens och det nya dataskyddsdirektivets reglering om konsekvensbedömning.

Behovet av en konsekvensbedömning vid kamerabevakning innebär i och för sig en nyhet jämfört med vad som gäller i dag. Av artikel 35.1 i dataskyddsförordningen framgår emellertid att en konsekvensbedömning kan omfatta en serie av liknande behandlingar som medför liknande höga risker. I skäl 92 till förordningen anges vidare att det ibland kan vara förnuftigt och ekonomiskt att en konsekvensbedömning avseende dataskydd inriktar sig på ett vidare område än ett enda projekt. Även av de riktlinjer som antagits av den så kallade artikel 29-grupppen framgår att en enda konsekvensbedömning kan användas för att bedöma flera behandlingar som liknar varandra (WP 248 rev.01). Enligt riktlinjerna kan så vara fallet när liknande teknik används för att samla in uppgifter för samma ändamål. Till exempel anges att en grupp kommunala myndigheter som var och en inför ett liknande övervakningssystem kan utföra en enda konsekvensbedömning. Ett annat exempel som anges i riktlinjerna är att en järnvägsoperatör kan täcka videoövervakning i samtliga tågstationer med en gemensam konsekvensbedömning. Eftersom artikel 27.1 i det nya dataskyddsdirektivet i huvudsak överensstämmer med artikel 35.1 i dataskyddsförordningen bör vad som nu anförs gälla även för sådana konsekvensbedömningar som krävs enligt direktivet.

Mot denna bakgrund bör exempelvis Polismyndigheten kunna ta fram en konsekvensbedömning som kan användas vid ett stort antal bevakningssituationer. I enlighet med vad som anförs i avsnitt 6.3 om förbättrade möjligheter att få tillstånd behöver en ansökan dessutom inte längre innehålla ett omfattande underlag med statistik över brottsligheten på den aktuella platsen i förhållande till brottslighet på andra jämförbara platser. En och samma tillståndsansökan bör vidare, precis som i dag, kunna omfatta kamerabevakning från flera rörliga objekt, t.ex. fordon eller drönare (jfr 8 § kameraövervakningsförordningen). Enligt regeringens bedömning kommer den administrativa bördan i samband med ett ansökningsförfarande för exempelvis Polismyndigheten därmed att bli mindre än i dag.

Regeringen delar *Datainspektionens* uppfattning att en tillståndsansökan också bör innehålla en hänvisning till den lag eller annan författning, kollektivavtal eller beslut som utgör den rättsliga grunden för kamerabevakningen. På så vis blir det tydligare för privata subjekt att de bara undantagsvis omfattas av tillståndsplikten samtidigt som det blir lättare för tillsynsmyndigheten att bedöma om tillståndskravet gäller i eventuella gränsfall. Enligt regeringens mening kan kravet i denna del

emellertid begränsas till att avse kamerabevakning som bedrivs av andra än myndigheter. Mot bakgrund av att en ansökan enligt vad som nu föreslås ska innehålla uppgift om de omständigheter i övrigt som är av betydelse för prövningen kan regeringen inte se något behov av att införa en möjlighet för tillsynsmyndigheten att meddela ytterligare föreskrifter om vad en ansökan ska innehålla.

Yttrande från kommunen – bara i undantagsfall

Enligt kameraövervakningslagen ska den kommun där övervakningen ska ske få tillfälle att yttra sig innan länsstyrelsen beslutar om tillstånd, om det inte är onödigt (18 §). Av den kartläggning som utredningen har gjort framgår att kommunerna sällan har några särskilda synpunkter samtidigt som deras hörande medför en viss tidsutdräkt i ärendena. Särskilt tydligt blir detta när tillståndsprövningen rör kamerautrustade drönare som ska användas i ett stort antal kommuner, ibland i hela landet.

I enlighet med vad bl.a. *Länsstyrelsen Västra Götalands län* framhåller är avsikten med att kommunerna ska ges tillfälle att yttra sig främst att säkerställa att eventuella kommunala aspekter och lokala synpunkter förs fram. Vikten av att tillämpningen är enhetlig över hela landet och den begränsade nyttan som yttranden från kommunen synes ha i dag talar för att detta krav helt borde tas bort. Det kan dock inte uteslutas att ett sådant yttrande kan vara värdefullt vid tillståndsprövningen i vissa fall. Möjligheten för tillsynsmyndigheten att inhämta ett yttrande från kommunen bör därför finnas kvar. Utredningen föreslår att den kommun där bevakningen ska ske ska få tillfälle att yttra sig om det behövs.

För att markera att detta framöver ska ske endast i undantagsfall, bör det enligt regeringens mening anges att berörd kommun ska få tillfälle att yttra sig, om det av särskild anledning behövs. En sådan anledning skulle t.ex. kunna vara om omfattande och varaktig bevakning ska ske av centrala stadsdelar eller bevakning ska ske av en plats där flera kommunala evenemang väntas äga rum.

Tillståndsbeslutet

Ett beslut om tillstånd ska enligt 19 § kameraövervakningslagen förenas med villkor om hur kameraövervakningen får anordnas. Sådana villkor ska avse övervakningens ändamål, den utrustning som får användas och det område som får övervakas. Länsstyrelserna ska också besluta om de övriga villkor som behövs för tillståndet. Sådana villkor får avse upplysningar om övervakningen, upptagning, användning, bevarande eller annan behandling av bilder, avlyssning eller upptagning av ljud samt andra förhållanden som har betydelse för att skydda enskildas personliga integritet. Enligt 20 § kameraövervakningslagen får ett beslut meddelas för en begränsad tid och länsstyrelserna får besluta om nya villkor eller återkalla tillståndet om förutsättningarna för tillståndet ändras.

Varken dataskyddsförordningen eller det nya dataskyddsdirektivet innehåller några bestämmelser om hur ett förhandstillstånd ska utformas. Det framstår därför som lämplig att en sådan reglering tas in i kamerabevakningslagen. Kameraövervakningslagens nuvarande bestämmelser om tillståndsbeslutet är förenliga med EU-regleringen och får anses ändamålsenliga även för tillståndsbeslut enligt

kamerabevakningslagen. Motsvarande bestämmelser bör därför tas in i den nya lagen. Vissa mindre sakliga och språkliga ändringar bör emellertid göras. En sådan förändring är att det bör anges uttryckligen att villkoren också kan avse den typ av område där bevakningen ska ske. Detta för att öka flexibiliteten vid kamerabevakning från rörliga objekt som exempelvis fordon och drönare. Sådana villkor kan också utformas på ett sätt som reglerar var bevakning inte får ske, t.ex. i närheten av bostadsbebyggelse eller friluftsområden om sådana behov inte finns.

Att tillståndsbeslut även fortsättningsvis bör innehålla villkor om den utrustning som får användas och var den får placeras behöver inte innebära att ett nytt tillstånd behöver sökas vid minsta förändring. Tillsynsmyndigheten bör inte föreskriva mer detaljerade villkor än vad som behövs för att exempelvis avgränsa ett visst bevakningsområde eller knyta tillståndsbeslutet till en viss typ av teknik. Utgångspunkten bör vara att en tillståndshavare i normalfallet ska ha ett visst utrymme att flytta eller byta ut kameror inom samma område, i vart fall så länge det inte innebär att integritetsriskerna ökar.

Regeringen delar inte *Datainspektionens* uppfattning att tillståndshavare bör vara skyldiga att anmäla ändrade förhållanden till tillståndsmyndigheten. Tillståndshavaren måste dock följa de villkor som föreskrivs i tillståndsbeslutet vilket kan innebära att det krävs en ny ansökan om tillstånd vid en förändring av exempelvis bevakningens ändamål.

Av dataskyddsförordningen följer att ett krav på förhandstillstånd av det aktuella slaget ska prövas av den myndighet som utses till nationell tillsynsmyndighet enligt förordningen. Det är därför inte aktuellt att som *Malmö kommun* föreslår överlåta prövningen till kommunerna.

6.5 Undantagen från tillståndskravet ska behållas och utvidgas

Regeringens förslag: Från kravet på tillstånd till kamerabevakning görs följande undantag som i huvudsak motsvarar sådan kameraövervakning som är undantagen från tillståndsplikten eller är tillåten efter anmälan enligt kameraövervakningslagen:

1. Kamerabevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning.
2. Viss kamerabevakning vid skyddsobjekt. Jämfört med den nuvarande regleringen utvidgas undantaget till att också avse sådana skyddsobjekt som avses i 5 § 5 skyddslagen (2010:305) liksom byggnader, andra anläggningar och områden som används för eller är avsedda för fredstida krishantering enligt 4 § 4 skyddslagen.
3. Kamerabevakning som Försvarsmakten bedriver från ett fordon, fartyg eller luftfartyg som ett led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan bevakning.
4. Kamerabevakning som Trafikverket bedriver av vägtrafik och vid betalstationer för trängselskatt och infrastrukturavgifter. Jämfört med den nuvarande regleringen utvidgas undantaget till att också avse sjötrafik vid en rörlig bro.

5. Viss kamerabevakning i en vägtunnel som bedrivs av någon annan tunnelhållare än trafikverket.

6. Viss kamerabevakning i en tunnelbanevagn och av en tunnelbanestation. Jämfört med den nuvarande regleringen utvidgas undantaget till att omfatta bevakning som har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott eller förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor.

7. Viss kamerabevakning som har samband med postverksamhet. Jämfört med den nuvarande regleringen utvidgas undantaget till att omfatta bevakning i samtliga lokaler där det bedrivs postverksamhet eller av området omedelbart utanför in- och utgångar till en sådan lokal.

8. Viss kamerabevakning i parkeringshus. Jämfört med den nuvarande regleringen utvidgas undantaget till att omfatta bevakning som har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott.

9. Kamerabevakning som sker för säkerheten i trafiken eller arbetsmiljön från ett fordon, en maskin eller liknande för att förbättra sikten för föraren eller användaren.

Undantagen från tillståndskravet ska inte innehålla några begränsningar avseende hur kameran ska vara monterad, vilken optik som får användas eller huruvida ljud får avlyssnas eller tas upp.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår dock ingen utvidgning av undantaget för kamerabevakning av skyddsobjekt.

Remissinstanserna: En majoritet av remissinstanserna, däribland *Datainspektionen*, tillstyrker förslaget eller har inga synpunkter på det. *Polismyndigheten* anser i första hand att varje kamerabevakning som är nödvändig och annars vore laglig enligt dataskyddsregleringen borde undantas från tillståndskravet. I vart fall anser Polismyndigheten att kameror som används i eller på fordon, fartyg eller luftfartyg eller liknande rörliga objekt bör undantas från tillståndskravet då det i sådana fall är lämpligare med ett förhandssamråd med tillsynsmyndigheten på systemnivå. *Säkerhetspolisen* föreslår att undantaget från tillståndskravet för kamerabevakning av skyddsobjekt utsträcks till att även omfatta ett område i skyddsobjektets närhet och inte enbart området i dess omedelbara närhet. Detta skulle enligt Säkerhetspolisen korrespondera bättre med de behov som finns och gränsen för skyddsvakternas befogenheter för att skydda objektet. *Myndigheten för samhällsskydd och beredskap (MSB)* anser att begränsningen av undantaget från tillståndskravet för kamerabevakning av sådana skyddsobjekt som används för eller är avsedda för fredstida krishantering enligt 4 § 4 skyddslagen bör tas bort. MSB ser stora tillämpningssvårigheter med att urskilja sådana skyddsobjekt från de skyddsobjekt som i övrigt avses i 4 § 4 skyddslagen. *Försvarsmakten* anser att undantaget från kravet på tillstånd även bör gälla för bevakning av ett sådant skyddsobjekt som avses i 5 § 5 skyddslagen, dvs. områden där ett Natohögkvarter eller en främmande stats militära styrka bedriver militär verksamhet inom ramen för samförståndsavtalet den 4 september 2014 mellan Sverige och Nato om värdlandsstöd. Försvarsmakten anser vidare att undantaget för Försvarsmaktens

kamerabevakning bör bli mer teknikneutralt. *Totalförsvarets forskningsinstitut (FOI)* anser att det bör klargöras att undantagen även omfattar sådan provning av utrustning som genomförs för Försvarsmaktens räkning, även om det inte är Försvarsmakten som bedriver provningen. När det gäller användningen av kamerautrustade drönare förespråkar flera remissinstanser, bl.a. *Transportstyrelsen*, *Lantmäteriet* och *Sjöräddningssällskapet*, någon form av undantag från tillståndskravet för myndigheter generellt. Detta främst för att underlätta för exempelvis tillsynsverksamhet, mätningar och annan verksamhet som endast i undantagsfall innebär risker för att människor filmas eller fotograferas. Transportstyrelsen och *Utredningen om självkörande fordon på väg (N 2015:07)* anser vidare att undantaget som tar sikte på kamerabevakning som sker för säkerheten i trafiken är för snävt utformat. Enligt den utredningen borde undantaget omfatta fler kameror än sådana som förbättrar sikten för föraren och i stället gälla generellt för bevakning som sker med en kamera som för ett säkert framförande i trafiken eller arbetsmiljön är uppsatt på ett fordon, en maskin eller liknande. *Trafikverket* anser att det är positivt att bevakning av sjötrafik vid en öppningsbar bro i anslutning till väg inte längre ska omfattas av tillståndskravet. Trafikverket anser dock att ytterligare undantag bör införas avseende järnvägs- och kollektivtrafik. Liknande synpunkter framförs av bl.a. *SJ AB*, *Svensk Kollektivtrafik* och *Jernhusen AB.* Enligt Polismyndigheten bör i vart fall sådan kollektivtrafik som kan jämföras med tunnelbana, exempelvis Citytunneln i Malmö, kunna undantas från tillståndskravet. *Stockholms läns landsting* instämmer i behovet av ett bredare undantag för kollektivtrafiken och föreslår också ett nytt undantag från tillståndskravet vid kamerabevakning inom vissa ytor och byggnader inom hälso- och sjukvården, exempelvis väntrum och entréer på akutmottagningar. *Postnord AB* välkomnar det bredare undantaget för postverksamhet.

Skälen för regeringens förslag

Regeringen instämmer i utredningens bedömning att de flesta av de nuvarande undantagen från tillståndsplikten i kameraövervakningslagen är ändamålsenliga också i förhållande till tillståndskravet i den nya kamerabevakningslagen. Viss kamerabevakning som tidigare varit undantagen från tillståndskravet kommer i enlighet med det mer begränsade tillståndskrav som ska gälla enligt kamerabevakningslagen dock inte längre att vara tillståndspliktig. Det innebär att vissa av de nuvarande undantagen har spelat ut sin roll. Så är exempelvis fallet med undantagen för övervakning i ett kasino (10 § första stycket 7) liksom sådan övervakning som efter anmälan får ske i en banklokal, vid uttagsautomater (12 § första stycket 1 och 2) och i butiker (13 §).

Att viss kamerabevakning inte längre omfattas av vare sig ett tillståndskrav eller en anmälningsplikt innebär inte att den blir oreglerad. Tvärtom kommer den i vissa avseenden att vara föremål för en mer omfattande reglering till skydd för den personliga integriteten än i dag (se avsnitt 6.2). Den som bedriver kamerabevakning som inte är föremål för ett tillståndskrav måste i första hand se till att kamerabevakningen är förenlig med regleringen i dataskyddsförordningen eller annan tillämplig

personuppgiftsreglering. I vissa fall kan sådan kamerabevakning t.ex. kräva en konsekvensbedömning avseende dataskydd och en skyldighet att samråda med tillsynsmyndigheten.

Undantagen från tillståndskravet behålls och utvidgas

De undantag från tillståndsplikten som finns i kameraövervakningslagen och som fortfarande är relevanta i förhållande till tillståndskravet i kamerabevakningslagen bör överföras till den nya lagen. Detta gäller dels de rena undantag från tillståndskravet som finns i 10 § kameraövervakningslagen och dels sådan kameraövervakning som är undantagen från tillståndskravet men kräver en anmälan i enlighet med 12–15 §§. Till den senare kategorin hör kameraövervakning i en tunnelbanevagn eller av en tunnelbanestation, i ett postkontor och i parkeringshus. De nu nämnda undantagen bör som utredningen föreslår också utvidgas något, bl.a. genom att fler syften anges uttryckligen i respektive undantagsbestämmelse, t.ex. syftet att lagföra brott.

Undantaget från tillståndskravet som avser kamerabevakning i en tunnelbanevagn och av en tunnelbanestation bör således omfatta kamerabevakning som har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott eller förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor. Undantaget som avser kamerabevakning i parkeringshus bör på motsvarande sätt omfatta bevakning som har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott. Även undantaget som avser kamerabevakning i postkontor bör knytas till dessa syften. I enlighet med vad utredningen föreslår bör det undantaget också breddas något genom att avse lokaler där det bedrivs postverksamhet. Utredningen föreslår dessutom att undantaget uttryckligen ska omfatta kamerabevakning av en yta i en butikslokal på vilken det bedrivs postverksamhet. Regeringen anser emellertid inte att det är nödvändigt eftersom sådana butikslokaler redan omfattas av formuleringen lokal där det bedrivs postverksamhet. Vad som är postverksamhet definieras i 1 kap. 2 § postlagen (2010:1045).

Undantagen från tillståndskravet bör i enlighet med utredningens förslag, inte innehålla några begränsningar avseende hur kameran ska vara monterad, vilken optik som får användas eller huruvida ljud får avlyssnas eller tas upp. Frågan om ljud får avlyssnas eller tas upp kommer därmed avgöras genom en tillämpning av annan tillämplig personuppgiftsreglering, t.ex. dataskyddsförordningen. Med hänsyn till det betydande integritetsintrång som avlyssning eller upptagning av ljud kan medföra torde utgångspunkten även fortsättningsvis vara att kamerabevakning i de aktuella fallen inte bör möjliggöra avlyssning eller inspelning av människors samtal.

Vissa skyddsobjekt är undantagna från tillståndskravet i kameraövervakningslagen. Enligt regeringens bedömning föreligger ett ökat behov av kamerabevakning i samhället på vissa strategiska platser. Det framstår därför, som *Myndigheten för samhällsskydd och beredskap (MSB)* framhåller, ändamålsenligt att undantaget för skyddsobjekt utvidgas till att även avse sådana byggnader, andra anläggningar och områden som enligt 4 § 4 skyddslagen används för eller är avsedda för

fredstida krishantering. I enlighet med vad *Försvarsmakten* anför bör undantag även göras för sådana skyddsobjekt som avses i 5 § 5 skyddslagen, dvs. områden där ett Natohögkvarter eller en främmande stats militära styrka bedriver militär verksamhet inom ramen för samförståndsavtalet den 4 september 2014 mellan Sverige och Nato om värdlandsstöd.

Säkerhetspolisen föreslår en utvidgning av det område som får bevakas i anslutning till ett skyddsobjekt för att korrespondera bättre med behovet av bevakning och skyddsvakternas befogenhet. Det saknas dock underlag för att göra en sådan utvidgning i detta lagstiftningsärende. Detta innebär att det tillståndsfria området runt ett skyddsobjekt kommer att vara begränsat till området i skyddsobjektets omedelbara närhet. Om det av särskild anledning föreligger en förhöjd hotbild mot det aktuella skyddsobjektet bör det dock finnas goda möjligheter att bevilja ett tillstånd för kamerabevakning av ett större område i enlighet med vad som framgår i avsnitt 6.3.

Kamerabevakning vid rörliga broar kan ha stor betydelse för att förhindra olyckor eller för att minska skadeverkningarna av inträffade olyckor. Enligt utredningen anses Trafikverkets nuvarande undantag från tillståndsplikten i kameraövervakningslagen inte omfatta bevakning av sjötrafik i samband med öppning och stängning av en rörlig bro. I enlighet med utredningens förslag bör därför Trafikverkets undantag utvidgas till att även gälla sjötrafik vid en rörlig bro.

Polismyndigheten föreslår i första hand att all myndighetens kamerabevakning som är nödvändig och laglig enligt dataskyddsregleringen ska undantas från tillståndskravet. Ett sådant undantag skulle i praktiken innebära att tillståndskravet för Polismyndighetens kamerabevakning tas bort. Det finns inte underlag att i detta lagstiftningsärende lämna ett sådant förslag men regeringen anser att det är angeläget att frågan utreds vidare (se avsnitt 6.2).

Regeringen anser inte heller att det är möjligt att för närvarande införa ett generellt undantag för Polismyndighetens användning av kamerabevakning med fordon eller drönare. Konsekvenserna av ett sådant undantag är inte närmare belysta av utredningen och därför svåra att överblicka. Utgångspunkten bör i stället vara att förbättra möjligheterna att få tillstånd också till sådan kamerabevakning som sker med hjälp av ett fordon eller en drönare. I enlighet med vad som framgår i avsnitt 6.4 bör en och samma ansökan med tillhörande gemensam konsekvensbedömning kunna omfatta en personuppgiftsansvarigs användning av kamerautrustade fordon eller drönare generellt. Förfarandet blir därmed i praktiken mycket likt ett sådant förhandssamråd på systemnivå som Polismyndigheten efterfrågar. När det gäller användning av kamerabevakning med fordon eller drönare av mer tillfällig karaktär föreslås dessutom både en förlängning och en utvidgning av Polismyndighetens och Säkerhetspolisens tillfälliga undantag (se avsnitt 6.6).

När det gäller användningen av kamerautrustade drönare förespråkar flera remissinstanser, bl.a. *Lantmäteriet* och *Sjöräddningssällskapet*, någon form av undantag från tillståndskravet för myndigheter generellt. Den främsta anledningen till ett sådant undantag skulle vara att underlätta för exempelvis tillsynsverksamhet, mätningar och annan verksamhet som

endast i undantagsfall innebär risker för att människor filmas eller fotograferas. Tillämpningsområdet för den nya lagen föreslås emellertid i avsnitt 5.3.3 bli snävare än tillämpningsområdet för kameraövervakningslagen. Det bör därigenom finnas goda förutsättningar att se till att användning av drönartekniken för de ovan angivna ändamålen inte innebär en varaktig eller regelbundet upprepad personbevakning. I sådana fall blir den nya lagen inte tillämplig. Enligt regeringens bedömning är därför behovet av ett särskilt undantag i lagen från tillståndsplikten vid användning av kamerautrustade drönare litet. Det finns samtidigt betydande integritetsrisker med tekniken om den används på ett sätt som innebär personbevakning. Något generellt undantag från tillståndskravet för myndigheters användning av kamerautrustade drönare bör därför inte införas.

Den nya lagens snävare tillämpningsområde bör även medföra att sådan användning av kameror som exempelvis *Försvarsmakten* har behov av oftare kommer att falla utanför lagens tillämpningsområde. Det finns mot den bakgrunden inte skäl att justera Försvarsmaktens nuvarande undantag från tillståndskravet enligt myndighetens önskemål. Även *Totalförsvarets forskningsinstitut (FOI)* bör ha bättre möjligheter att prova utrustning för Försvarsmaktens räkning utan att omfattas av den nya lagens tillämpningsområde. Den typ av provverksamhet som FOI bedriver förväntas nämligen inte uppfylla den nya lagens krav på varaktig eller regelbundet upprepad personbevakning.

Undantagen från tillståndskravet är som FOI uppmärksammar ofta kopplade till att en viss aktör bedriver bevakningen. Vem som ska anses bedriva bevakningen måste avgöras från fall till fall och det finns inget hinder mot att den som bedriver bevakningen anlitar någon annan att faktiskt utföra bevakningen (se bl.a. prop. 2012/13:115 s. 57). Det är således möjligt för Försvarsmakten att anlita någon annan att utföra bevakningen för myndighetens räkning. Det aktuella undantaget bör mot denna bakgrund även fortsättningsvis avse sådana fall där Försvarsmakten ska anses bedriva bevakningen.

När det gäller undantaget i kameraövervakningslagen som tar sikte på bevakning som sker för säkerheten i trafiken anser bl.a. *Transportstyrelsen* att det är för snävt utformat. Enligt det undantaget gäller tillståndskravet inte för sådana kameror som för säkerheten i trafiken eller arbetsmiljön är uppsatt på ett fordon, en maskin eller liknande för att förbättra sikten för föraren eller användaren. Undantaget omfattar exempelvis sådana backkameror som aktiveras när föraren backar fordonet och hjälper föraren att manövrera fordonet på ett trafiksäkert sätt. Att i nuläget utvidga det aktuella undantaget till att t.ex. omfatta all sådan kamerateknik som kan krävas vid användning av självkörande fordon skulle innebära en betydande utvidgning. Det saknas underlag för att lägga fram ett sådant förslag i detta lagstiftningsärende. Det kan dock konstateras att kamerabevakningslagens tillståndskrav inte kommer att gälla för de flesta privaträttsliga subjekt som använder självkörande fordon. *Utredningen om självkörande fordon på väg (N 2015:07)* har dessutom i uppdrag att överväga och lämna författningsförslag i syfte att skapa bättre rättsliga förutsättningar för försök med självkörande fordon i allmän trafik och för introduktion av sådana fordon i allmän trafik (dir. 2015:114). Utredningen ska redovisa sitt uppdrag senast den 1 mars 2018.

Flera remissinstanser, däribland *Stockholms läns landsting*, *SJ AB* och *Jernhusen AB*, förespråkar att undantaget för tunnelbanevagnar och tunnelbanestationer utvidgas till att omfatta i princip all järnvägs- och kollektivtrafik. Det kan först konstateras att det undantag för tunnelbanestationer som nu föreslås också är avsett att omfatta områden innanför stationens spärrlinje som är avsedda för annan spårbunden trafik, exempelvis pendeltåg. Enligt regeringens uppfattning finns det goda argument för att därtill införa ett utökat undantag från tillståndskravet för järnvägs- och kollektivtrafik. Det finns emellertid inte underlag att behandla frågan i detta lagstiftningsärende. Den utredning om förenklade möjligheter till kameraövervakning som regeringen har tillsatt har dock fått i uppdrag att analysera om ett utökat undantag från tillståndsplikten för kameraövervakning av allmänna transportmedel och stationer bör införas (dir. 2017:124). Regeringen avser alltså att återkomma i frågan. Det bör också framhållas att den nya kamerabevakningslagen kommer innebära förbättrade möjligheter att få tillstånd vid kamerabevakning av övriga allmänna transportmedel och stationer för brottsbekämpande och trygghetsskapande syften (se avsnitt 6.3).

Det saknas underlag att i detta sammanhang närmare överväga ett undantag från tillståndskravet för viss kamerabevakning inom hälso- och sjukvården. Möjligheterna att få tillstånd för kamerabevakning på platser av det aktuella slaget där det finns problem med brottslighet och andra störningar kommer dessutom att förbättras genom regeringens förslag eftersom det vid tillståndsprövningen ska beaktas särskilt om kamerabevakningen behövs för att platsen är brottsutsatt eller för att det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet till person eller på egendom (se avsnitt 6.3).

6.6 Även de tillfälliga undantagen ska behållas och utvidgas

Regeringens förslag: Från kravet på tillstånd till kamerabevakning görs följande tillfälliga undantag som i huvudsak motsvarar de tillfälliga undantagen från tillståndsplikten enligt kameraövervakningslagen:

1. Viss kamerabevakning som bedrivs av Polismyndigheten eller Säkerhetspolisen i samband med risk för allvarlig brottslighet. Jämfört med den nuvarande regleringen förlängs undantaget till att gälla under högst tre månader. Undantaget utvidgas dessutom till att omfatta alla typer av allvarlig brottslighet och även innefatta kamerabevakning som sker i syfte att upptäcka sådan brottslighet eller utreda eller lagföra sådana brott.
2. Viss kamerabevakning som bedrivs av Polismyndigheten eller den som är räddningsledare i samband med olyckor. Jämfört med den nuvarande regleringen utvidgas undantaget till att även omfatta bevakning i syfte att minska risken för nya olyckor.
3. Kamerabevakning som bedrivs av den som är räddningsledare om bevakningen är av vikt för att efterforska en försvunnen person.

Om en ansökan om tillstånd görs inom den föreskrivna tiden ska bevakningen få bedrivas utan tillstånd till dess att ansökan har prövats.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår dock att det tillfälliga undantaget för Polismyndigheten och Säkerhetspolisen ska gälla under högst en månad och fortsätta vara begränsat till vissa angivna typer av allvarlig brottslighet. Utredningen föreslår inte någon utvidgning av undantaget som rör räddningsinsatser.

Remissinstanserna: En majoritet av remissinstanserna tillstyrker förslaget eller har inga synpunkter på det. *Polismyndigheten* anser att det nuvarande rekvisitet allvarlig brottslighet i det tillfälliga undantaget borde bytas ut mot brottslighet. Detta eftersom sådan brottslighet som enskilt inte når upp till rekvisitet allvarlig brottslighet men som sammantaget utgör en betydande belastning på samhället, t.ex. narkotikahandel, återkommande hot- och skadegörelse, sexuella ofredanden under festivaler, stölder och eldning av bilar inte kan bekämpas med de nuvarande eller föreslagna tillfälliga undantagen. Det tidsbegränsade undantagen bör enligt Polismyndigheten i vart fall omfatta längre tid än vad som nu är fallet, förslagsvis sex månader, innan en ansökan om tillstånd behöver göras. Även *Malmö kommun* efterlyser ett längre tidsbegränsat undantag för Polismyndigheten. *Tullverket* anser att myndigheten också bör omfattas av det tillfälliga undantaget från tillståndskravet för Polismyndigheten och Säkerhetspolisen. Detta då Tullverket inte sällan hanterar organiserad brottslighet med bl.a. grov narkotikasmuggling. Enligt Tullverket skulle motsvarande möjligheter dessutom underlätta samarbetet mellan de berörda myndigheterna i arbetet mot den organiserade brottsligheten. *Myndigheten för samhällsskydd och beredskap (MSB)* föreslår att det tillfälliga undantaget från tillståndskravet i föreslagna 11 § första stycket 2 och 3 utformas mer generellt för att omfatta alla räddningsinsatser enligt 1 kap. 2 § lagen om skydd mot olyckor. MSB bedömer att det finns ett värde av att undantagen utvidgas till att även avse efterföljande åtgärder enligt 3 kap. 9 § och 4 kap. 7 § lagen om skydd mot olyckor med hänsyn till risken för nya olyckor. Sådan efterbevakning skulle vara särskilt värdefull vid större skogsbränder. *Kustbevakningen* efterlyser förtydliganden om undantagen även gäller när Kustbevakningen biträder de angivna myndigheterna eller en räddningsledare i aktuella situationer. *Sveriges Kommuner och Landsting* anser att det också finns skäl för att utvidga de aktuella undantagen till att även omfatta en sådan ambulans- och akutsjukvårdsinsats som utförs inom hälso- och sjukvården och som inte bedrivs av en räddningsledare enligt lagen om skydd mot olyckor. *Stockholms läns landsting* anser att användning av exempelvis drönare som en del i en vård- och behandlingsåtgärd inom ramen för hälso- och sjukvårdslagen eller smittskyddslagen (2004:168) borde vara undantagen från tillståndsplikten på samma sätt som vid räddningsinsatser enligt lagen om skydd mot olyckor.

Skälen för regeringens förslag

I 11 § kameraövervakningslagen finns tillfälliga undantag från tillståndskravet som innebär att vissa subjekt får bedriva kameraövervakning för vissa specifika och angelägna ändamål under en

månads tid utan att en ansökan om tillstånd har gjorts. Om ansökan om tillstånd görs inom en månad från det att övervakningen inleds får övervakningen dessutom bedrivas utan tillstånd till dess att ansökningen har prövats. Undantagen avser 1) övervakning som bedrivs av Polismyndigheten eller den som är räddningsledare enligt lagen om skydd mot olyckor, om övervakningen är av vikt för att avvärja en hotande olycka eller för att begränsa verkningarna av en inträffad olycka, 2) övervakning som bedrivs av den som är räddningsledare enligt lagen om skydd mot olyckor, om övervakningen är av vikt för att efterforska en försvunnen person, och 3) övervakning som bedrivs av Polismyndigheten eller Säkerhetspolisen, om det av särskild anledning finns risk för att allvarlig brottslighet som innebär fara för liv eller hälsa eller för omfattande förstörelse av egendom kommer utövas på en viss plats och syftet med övervakningen är att förebygga och förhindra brott.

Regeringen anser att samtliga tillfälliga undantag i kameraövervakningslagen är relevanta också i förhållande till tillståndskravet i kamerabevakningslagen. Undantagen bör därför behållas. Det bör dessutom övervägas om något eller några av undantagen ska utvidgas för att underlätta ytterligare för angelägen kamerabevakning av tillfällig karaktär.

Undantaget för Polismyndigheten och Säkerhetspolisen vid allvarlig brottslighet bör förlängas och utvidgas

Ett av de tillfälliga undantagen i 11 § kameraövervakningslagen tar sikte på sådan övervakning som bedrivs av Polismyndigheten eller Säkerhetspolisen. Undantaget är tillämpligt om det av särskild anledning finns risk för att allvarlig brottslighet som innebär fara för liv eller hälsa eller för omfattande förstörelse av egendom kommer utövas på en viss plats och syftet med övervakningen är att förebygga eller förhindra brott. Övervakning med stöd av undantaget får ske under högst en månad utan att en ansökan om tillstånd har gjorts Undantaget kan tillämpas för att tillfälligt kamerabevaka på platser där det av särskild anledning finns risk för exempelvis allvarliga våldsbrott, systematiska fall av sexuella övergrepp eller eldning av bilar och har bl.a. använts av Polismyndigheten i samband med uppsättandet av kameror i vissa områden med grov gängkriminalitet (se bl.a. Länsstyrelsen i Stockholms läns beslut 2017-11-10, 2112-24799-2017).

Som utredningen föreslår bör det nuvarande undantaget utvidgas till att också innefatta sådan kamerabevakning som sker i syfte att upptäcka sådan brottslighet som omfattas av undantaget, eller utreda eller lagföra sådana brott. Det blir därmed tydligt att undantaget är tillämpligt även när den brottspreventiva effekten förväntas vara låg eller obefintlig om bevakningen kan bidra till att brott kan upptäckas, utredas och lagföras. Begreppet utreda och lagföra brott syftar precis som i andra bestämmelser i kamerabevakningslagen på brott som ännu inte har begåtts och inte på arbetet i en pågående förundersökning.

Polismyndigheten anser att undantaget bör utvidgas till att avse all brottslighet inte bara viss allvarlig brottslighet. En sådan utvidgning skulle i praktiken innebära ett heltäckande undantag, om än tidsbegränsat, från tillståndskravet för Polismyndighetens och Säkerhetspolisens

kamerabevakning i den brottsbekämpande verksamheten. Frågan om så pass omfattande undantag från tillståndskravet bör övervägas inom ramen för den pågående utredningen på området (dir. 2017:124).

Enligt regeringens mening bör dock undantaget redan nu kunna utvidgas för att möjliggöra tillfällig kamerabevakning i flera av de fall som Polismyndigheten efterfrågar. Till skillnad mot vad utredningen föreslår bör undantaget därför inte längre vara begränsat till vissa typer av allvarlig brottslighet utan omfatta allvarlig brottslighet generellt. Detta innebär att undantaget kan tillämpas även vid kamerabevakning av exempelvis platser med omfattande narkotikahandel. Det bör i sammanhanget också framhållas att det inte krävs en misstanke om ett visst konkret brott för att undantaget ska vara tillämpligt utan det räcker med att det av särskild anledning finns risk för allvarlig brottslighet.

Regeringen anser i likhet med Polismyndigheten att det även finns skäl att förlänga tiden för det aktuella undantaget. Detta skulle medföra minskad administration, ökad flexibilitet och en klar förbättring av Polismyndighetens och Säkerhetspolisens möjligheter att i särskilt angelägna fall bedriva kamerabevakning utan att i förväg behöva söka tillstånd. Enligt regeringen bör den tid som anges i undantaget utsträckas till tre månader.

En utvidgning av det aktuella undantaget från en till tre månader innebär bl.a. förbättrade möjligheter för Polismyndigheten och Säkerhetspolisen att i händelse av ett förhöjt terrorhot snabbt sätta in kamerabevakning på strategiska platser under en längre men ändå begränsad tid. Det blir också lättare att bedriva kamerabevakning av en viss plats vid flera på varandra följande publika evenemang, t.ex. under sommarmånaderna. Att kamerabevakning kan bedrivas tillståndsfritt under tre månader i stället för en månad ger dessutom myndigheterna nya möjligheter att utvärdera och använda erfarenheter från den tillfälliga bevakningen i tillståndsförfarandet för att visa på behovet av en mer varaktig kamerabevakning.

Undantaget bör även fortsättningsvis vara förbehållet Polismyndigheten och Säkerhetspolisen. Vad *Tullverket* anför om att myndigheten också bör undantas bör i stället övervägas inom ramen för den pågående utredningen om förenklade möjligheter till kameraövervakning.

Mot denna bakgrund bör undantaget som innebär att Polismyndigheten eller Säkerhetspolisen i vissa fall får bedriva kamerabevakning utan att en ansökan om tillstånd har gjorts utvidgas från att gälla under högst en månad till att gälla under högst tre månader. Undantaget ska dessutom omfatta alla typer av allvarlig brottslighet och även innefatta sådan kamerabevakning som sker i syfte att upptäcka sådan brottslighet eller utreda eller lagföra sådana brott.

Räddningsinsatser och skydd mot olyckor

I 11 § kameraövervakningslagen finns också tillfälliga undantag som tar sikte på övervakning vid olyckor respektive vid efterforskandet av försvunna personer. Även dessa undantag har en övre tidsgräns på en månad innan en ansökan måste göras. Enligt det ena undantaget får övervakning under denna tid bedrivas utan tillstånd av den som är räddningsledare enligt lagen om skydd mot olyckor, förkortad LSO, om

övervakningen är av vikt för att efterforska en försvunnen person. Enligt det andra undantaget får övervakning bedrivas av Polismyndigheten eller den som är räddningsledare enligt lagen om skydd mot olyckor, om övervakningen är av vikt för att avvärja en hotande olycka eller för att begränsa verkningarna av en inträffad olycka.

I enlighet med vad *Myndigheten för samhällsskydd och beredskap (MSB)* anför finns anledning att anpassa undantaget ytterligare till regleringen i lagen om skydd mot olyckor. Det bör bl.a. tydliggöras att även sådan kamerabevakning som sker vid efterföljande åtgärder i samband med olyckor för att minska risken för nya olyckor omfattas av undantaget. Sådan efterbevakning kan som MSB framhåller vara särskilt värdefull vid större skogsbränder. Även i övrigt bör en viss språklig anpassning av begreppen ske till regleringen i lagen om skydd mot olyckor.

En räddningsledare får anses ansvarig för kamerabevakningen även om den utförs av en myndighet eller kommun som lämnar biträde enligt 6 kap. 7 § LSO. Den myndighet eller kommun som lämnar biträde får alltså anses utföra övervakningen för räddningsledarens räkning (se prop. 2012/13:115 s. 57). Detta innebär att undantaget från tillståndsplikten är tillämpligt om exempelvis Kustbevakningen biträder räddningsledaren med kamerabevakning. Motsvarande får anses gälla i de fall en myndighet biträder Polismyndigheten.

Några remissinstanser, bl.a. *Stockholms läns landsting*, efterfrågar ytterligare tillfälliga undantag som bl.a. omfattar drönare som används som en del i en vård- och behandlingsåtgärd. Det saknas dock närmare utredning om vilka behov som finns av detta och hur ett sådant undantag i så fall skulle avgränsas. Det bör i sammahaget framhållas att kamerabevakningslagen får ett snävare tillämpningsområde än kameraövervakningslagen. Det innebär att endast sådan användning av kameror som innebär en varaktig eller regelbundet upprepad personbevakning kommer att omfattas av tillämpningsområdet och tillståndskravet.

Sammanfattningsvis bör undantaget som innebär att Polismyndigheten eller den som är räddningsledare enligt lagen om skydd mot olyckor i vissa fall får bedriva kamerabevakning utan att en ansökan om tillstånd har gjorts utvidgas till att även omfatta bevakning i syfte att minska risken för nya olyckor.

7 Upplysning om kamerabevakning

7.1 Ett särskilt upplysningskrav vid kamerabevakning

Regeringens förslag: Upplysning om kamerabevakning ska lämnas genom tydlig skyltning eller på annat verksamt sätt.

Om ljud kan avlyssnas eller tas upp vid bevakningen, ska en särskild upplysning lämnas om detta.

Enskildas rätt till information om den personuppgiftsbehandling som kamerabevakningen innebär ska regleras av bestämmelser i EU:s dataskyddsförordning och annan tillämplig personuppgiftsreglering.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår att det ska preciseras vilken information som ska lämnas genom tydlig skyltning eller på annat liknande verksamt sätt, bl.a. identiteten hos och kontaktuppgifter till den som bedriver bevakningen samt kontaktuppgifter till eventuellt dataskyddsombud. Utredningen föreslår också att viss annan information, bl.a. ändamålet och grunden för kamerabevakningen, ska göras tillgänglig för dem som kan bli kamerabevakade.

Remissinstanserna: Enligt *Datainspektionen* kan de särskilda förhållanden vid kamerabevakning – särskilt när den sker från t.ex. drönare – göra det svårt att helt uppfylla kraven på information i dataskyddsförordningen och det nya dataskyddsdirektivet. Eftersom det inte är möjligt att ha en bestämmelse om upplysningsskyldighet i kamerabevakningslagen som begränsar rätten till information enligt EU-regleringen avstyrker Datainspektionen förslaget. *Karlskrona kommun* anser att det är angeläget att ett upplysningskrav införs i den svenska lagen så att den som blir föremål för kameraövervakning blir informerad om detta på ett tydligt sätt. *Länsstyrelsen i Östergötland* anser också att det krävs en särskild reglering i kamerabevakningslagen om vilken information som ska lämnas eftersom den information som ska lämnas enligt EU-regleringen är omfattande. *Sveriges advokatsamfund* anser att upplysningskravet är viktigt och att dess föreslagna utformning är väl avvägd. Advokatsamfundet framhåller vidare att det inte bör vara tillåtet att sätta upp skyltar med upplysning när kamerabevakning inte förekommer, eftersom effekterna av en sådan skyltning i många fall kan vara lika integritetskränkande som när kamerabevakning faktiskt pågår. *Sjöräddningssällskapet* framhåller att det blir praktiskt komplicerat att upplysa om kamerabevakning vid flygningar över vatten i skiftande områden men att verksamheten i så fall torde kunna åberopa något av de föreslagna undantagen. *Sveriges byggindustrier* efterfrågar fler exempel på hur upplysningskravet ska följas i praktiken. *Malmö kommun* anser att förslaget behöver kompletteras med en tydlig reglering om var upplysningsskyltar ska placeras i förhållande till en kamera. Flera remissinstanser, däribland *Polismyndigheten*, *Trafikverket*, *Svensk handel*, *Lantbrukarnas riksförbund och Jägarnas riksförbund*, anser att det föreslagna upplysningskravet är för omfattande, särskilt när det gäller kontaktuppgifter till enskilda personer. Detta riskerar enligt flera av dessa remissinstanser att leda till hot och trakasserier. Dessutom framhålls att skyltar måste specialtillverkas och bytas ut, exempelvis om ett byte av dataskyddsombud sker. Jägarnas riksförbund föreslår att viltbevakningskameror i första hand undantas från kravet på skyltning eftersom de annars lätt blir ett eftertraktat stöldgods. *Svenska Jägareförbundet* anför att en person skulle kunna uppge sitt jägar-ID enligt Naturvårdsverkets jaktkortsregister som identifikation på upplysningen vid kamerabevakningen i stället för sitt namn. Enligt *Säkerhetspolisen* bör det räcka med att kontaktuppgifter till enskilda fysiska personer görs tillgängliga genom upplysningar på exempelvis myndighetens webbplats.

Naturvårdverket konstaterar att det föreslagna kravet på upplysning innebär att ganska omfattande information ska lämnas av en privatperson vid användning av viltkameror, till exempel för inventering eller bevakning av en åtel.

Skälen för regeringens förslag: Enligt 25 § kameraövervakningslagen ska som huvudregel upplysning om kameraövervakning lämnas genom tydlig skyltning eller på något annat verksamt sätt. Upplysning ska också lämnas om vem som bedriver övervakningen om detta inte framgår av förhållandena på platsen. Upplysningsplikten inträder redan när kameran sätts upp och är alltså inte beroende av om kameran används. Om ljud kan avlyssnas eller tas upp vid övervakningen ska en särskild upplysning lämnas om detta och den som bedriver övervakning ska också lämna upplysning om ändamålen med övervakningen, om den övervakade eller den som kan komma att bli övervakad begär det.

Dataskyddsförordningen och det nya dataskyddsdirektivet innehåller en omfattande reglering av de registrerades rättigheter. En av dessa rättigheter är rätten att få information från den personuppgiftsansvarige om personuppgiftsbehandling. Såväl förordningen som direktivet innehåller krav på vilken information som ska lämnas till den enskilde i olika situationer samt bestämmelser om hur detta ska ske.

Enligt dataskyddsförordningen (artiklarna 13 och 14) ska den enskilde som huvudregel bl.a. få information om den personuppgiftsansvariges identitet och kontaktuppgifter, om dataskyddsombudets kontaktuppgifter i tillämpliga fall samt om ändamålen med och den rättsliga grunden för behandlingen. Utöver detta ska den enskilde bl.a. få information om rätten att inge klagomål till tillsynsmyndigheten. Motsvarande reglering finns i det nya dataskyddsdirektivet (artiklarna 12 och 13) och kommer att genomföras i svensk rätt genom brottsdatalagen. I direktivet görs däremot skillnad på sådan allmän information som ska göras tillgänglig för den registrerade (artikel 13.1) och sådan information som i specifika fall ska lämnas till den registrerade (artikel 13.2).

Kamerabevakning skiljer sig från övrig personuppgiftsbehandling eftersom enskilda i praktiken måste upplysas om personuppgiftsbehandlingen i förväg. I många fall skulle det vara förenat med betydande integritetsrisker och dessutom i princip omöjligt för den som bedriver kamerabevakningen att gå igenom upptaget material och försöka hitta och informera berörda personer i efterhand. Vid användning av kamerautrustade drönare kan det finnas praktiska svårigheter även med att i förväg informera människor som kan komma att bli fångade på bild. Detta innebär, som *Datainspektionen* framhåller, att det kan vara svårt att fullt ut uppfylla EU-regleringens krav på information vid vissa typer av kamerabevakning. Samtidigt bör framhållas att EU-regleringen ger viss flexibilitet när det gäller den information som ska lämnas. Exempelvis behöver information inte lämnas, enligt dataskyddsförordningen, i den mån den registrerade redan förfogar över informationen (se artikel 13.4 och artikel 14.5). Således bör det finnas ett utrymme att inte lämna information om vem som bedriver övervakningen om det framgår av förhållandena på platsen (jfr 25 § kameraövervakningslagen).

Från integritetssynpunkt är det som bl.a. *Karlskrona kommun* framhåller viktigt att den som blir bevakad informeras om bevakningen på ett tydligt sätt. Detta möjliggör för enskilda att anpassa sig till att platsen är

kamerabevakad och, i många fall, välja om de vill bli föremål för sådan övervakning. Att bevakningen är känd är också av avgörande betydelse för att den ska vara effektiv i brottsförebyggande syfte. Det bör därför även fortsättningsvis som huvudregel gälla en upplysningsplikt vid kamerabevakning. Enligt regeringens bedömning är det möjligt att i nationell rätt ställa upp ett krav på upplysning som är kopplat till användningen av kameratekniken och inte direkt till behandlingen av personuppgifter. Detta hindrar inte att den som bedriver kamerabevakning genom upplysningen om kamerabevakning normalt sett också, helt eller delvis, uppfyller kravet på information enligt dataskyddsregleringen.

Frågan är då om det är möjligt och önskvärt att närmare reglera vad en sådan upplysning om kamerabevakning ska innehålla. Utredningen bedömer att en del av den information som ska lämnas enligt EU-regleringen inte är ändamålsenlig eller är praktiskt svår att lämna vid just kamerabevakning. Därför föreslår utredningen en särskild bestämmelse som reglerar vilken information om personuppgiftsbehandling som ska lämnas. Utredningens förslag innebär att viss information ska lämnas genom tydlig skyltning eller på något annat liknande verksamt sätt. Detta gäller bl.a. upplysning om själva kamerabevakningen, identiteten hos och kontaktuppgifterna till den som ska bedriva bevakningen och kontaktuppgifter till ett eventuellt dataskyddsombud. Förslaget innebär vidare att viss annan information ska göras tillgänglig för dem som kan bli kamerabevakade. Detta gäller bl.a. ändamålet med behandlingen och hur länge upptaget material får behandlas.

Utredningens förslag innebär en begränsning av rätten till information enligt den unionsrättsliga dataskyddsregleringen. Regeringen delar *Datainspektionens* uppfattning att dataskyddsförordningen inte ger utrymme för en sådan generell begränsning av den registrerades rätt till information vid kamerabevakning. Det kan vidare konstateras att utredningens förslag i vissa avseenden också innebär strängare krav än vad som följer av EU-rätten. Som anges ovan ger nämligen dataskyddsförordningen utrymme för att underlåta att lämna information i vissa fall, t.ex. i fråga om sådant som den registrerade redan känner till. Dessa undantag finns dock inte med i utredningens förslag och det kan ifrågasättas om detta är förenligt med EU-rätten. Det finns dessutom andra skäl som talar emot en svensk bestämmelse om vilken information som måste lämnas på en skylt eller på ett annat verksamt sätt. Som bl.a. *Polismyndigheten* och *Jägarnas Riksförbund* framhåller kan krav på att skylten ska innehålla kontaktuppgifter medföra risker för hot och trakasserier i vissa fall. Detaljerade krav om vilken information som ska lämnas vid skyltning kan också medföra att skyltar måste tillverkas speciellt för varje aktör som bedriver kamerabevakning och ett återkommande behov av att byta ut skyltarna, exempelvis vid ett byte av dataskyddsombud.

Mot denna bakgrund bör kravet på upplysning utformas på ett delvis annat sätt än vad utredningen föreslår. I lagen bör endast införas ett krav på att upplysning ska ske om kamerabevakningen, dvs. att platsen är kamerabevakad. Om ljud kan avlyssnas eller tas upp vid bevakningen bör det liksom i dag krävas att en särskild upplysning lämnas också om detta. Frågan om vilken information som ska lämnas om den personuppgiftsbehandling som kamerabevakningen innebär, t.ex. uppgift

om vem som bedriver kamerabevakningen, bör däremot i stället styras av bestämmelser i dataskyddsförordningen, brottsdatalagen och annan tillämplig personuppgiftslagstiftning. Detta bör framgå av en upplysningsbestämmelse i lagen. Som utredningen konstaterar kan skyltning på platsen även i fortsättningen förväntas bli ett vanligt sätt att uppfylla lagens upplysningskrav. Detta utesluter dock inte att upplysningsplikten kan uppfyllas även på andra sätt. Regeringen anser därför att upplysning om kameraövervakningen ska ske genom tydlig skyltning eller på något annat verksamt sätt.

Flera remissinstanser, bl.a. *Sveriges byggindustrier* och *Malmö kommun*, efterlyser förtydliganden om hur upplysning om kamerabevakning ska ske i praktiken. Enligt regeringens bedömning bör det många gånger vara lämpligt att lämna förhållandevis begränsad information om kamerabevakningen på en skylt i anslutning till platsen som bevakas samtidigt som övrig information som ska lämnas enligt bl.a. dataskyddsförordningen eller brottsdatalagen görs tillgänglig för den registrerade på annat sätt, t.ex. på en webbsida. I detta sammanhang bör också sådana uppförandekoder som regleras i artikel 40 i dataskyddsförordningen kunna vara till nytta. Enligt den regleringen ska bl.a. tillsynsmyndigheterna uppmuntra utarbetandet av särskilda uppförandekoder avsedda att bidra till att förordningen genomförs korrekt, med hänsyn till särdragen hos de olika sektorer där behandling sker. Regleringen innebär att olika branscher har möjlighet att utarbeta uppförandekoder som ska ges in till tillsynsmyndigheten för bedömning och godkännande. Även i övrigt bör de nationella tillsynsmyndigheterna inom ramen för de mekanismer som finns i dataskyddsförordningen ha goda möjligheter att uppnå ett gemensamt synsätt på hur information ska lämnas vid kamerabevakning.

Sveriges advokatsamfund föreslår att det ska införas ett förbud mot att skylta om kamerabevakning när sådan bevakning inte förekommer. Regeringen anser dock inte att det finns skäl att i kamerabevakningslagen införa regler som tar sikte på fall där personuppgifter inte behandlas överhuvudtaget.

7.2 Undantag från upplysningskravet och rätten till information

Regeringens förslag: Upplysning om kamerabevakning och information om den personuppgiftsbehandling som kamerabevakningen innebär ska inte behöva lämnas vid

1. bevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning,
2. bevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller Säkerhetspolisen, om det av särskild anledning finns risk för allvarlig brottslighet och syftet med bevakningen är att förebygga, förhindra eller upptäcka sådan brottslig verksamhet eller utreda eller lagföra sådana brott,
3. bevakning som sker för att skydda en byggnad, en annan anläggning eller ett område som enligt 4 § 4, 5 § 1–5 eller 6 § första

stycket skyddslagen har förklarats vara skyddsobjekt, om bevakningen endast omfattar skyddsobjektet eller ett område i dess omedelbara närhet,

4. bevakning som Försvarsmakten bedriver från ett fordon, fartyg eller luftfartyg som ett led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan bevakning,

5. bevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller den som är räddningsledare enligt lagen om skydd mot olyckor, om bevakningen är av vikt för att avvärja en överhängande fara för olycka, begränsa verkningarna av en inträffad olycka eller minska risken för nya olyckor, och

6. bevakning som bedrivs av den som är räddningsledare enligt lagen om skydd mot olyckor, om bevakningen är av vikt för att efterforska en försvunnen person.

Undantagen ska inte gälla, om ljud ska avlyssnas eller tas upp vid kamerabevakningen.

Om det finns synnerliga skäl, ska tillsynsmyndigheten i enskilda fall få besluta om undantag från upplysningskravet och rätten till information om den personuppgiftsbehandling som kamerabevakningen innebär. En ansökan om undantag ska vara skriftlig. Om bevakningen avser en arbetsplats, ska ett yttrande från ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på arbetsplatsen lämnas in tillsammans med ansökan. Den kommun där kamerabevakningen ska ske ska få tillfälle att yttra sig, om bevakningen ska avse en plats dit allmänheten har tillträde och det av särskild anledning behövs ett yttrande. Ett beslut om undantag ska förenas med de villkor som behövs och dess giltighet få begränsas till en viss tid. Om förutsättningarna för ett beslut om undantag ändras ska tillsynsmyndigheten få besluta om nya villkor, eller, om förutsättningarna för ett sådant beslut inte längre är uppfyllda, återkalla beslutet.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår ingen utvidgning av det nuvarande undantaget för skyddsobjekt. Utredningens förslag till undantag för Polismyndigheten och Säkerhetspolisen är begränsat till situationer där det av särskild anledning finns risk för vissa angivna typer av allvarlig brottslighet på en viss plats.

Remissinstanserna: En majoritet av remissinstanserna, däribland *Datainspektionen*, *Försvarets radioanstalt* och *Tjänstemännens Centralorganisation (TCO)*, tillstyrker förslaget eller har inga synpunkter på det. *Myndigheten för samhällsskydd och beredskap (MSB)* anser att undantaget från upplysningskravet för kamerabevakning i samband med olyckor ska utformas mer generellt och omfatta alla räddningsinsatser enligt 1 kap. 2 § lagen om skydd mot olyckor. MSB bedömer att det finns ett värde av att undantagen från upplysningskravet utvidgas till att även avse efterföljande åtgärder enligt 3 kap. 9 § och 4 kap. 7 § lagen om skydd mot olyckor med hänsyn till risken för nya olyckor. Sådan efterbevakning skulle vara särskilt värdefull bl.a. vid större skogsbränder. MSB ifrågasätter också begränsningen av undantaget som innebär att ljud inte får avlyssnas eller tas upp och framhåller att det ibland kan vara värdefullt

om räddningstjänsten kan uppfatta ljud som exempelvis ras, explosioner eller rop på hjälp. *Malmö kommun* anser att undantag från upplysningskravet också bör göras för sådana skyddsobjekt som används för eller är avsedda för fredstida krishantering. *Försvarsmakten* föreslår att den undantagsbestämmelse som rör Försvarsmaktens kamerabevakning görs teknikneutral. *Polismyndigheten* instämmer i utredningens slutsats att det inte alltid går att upplysa allmänheten om kamerabevakning i brådskade fall. Polismyndigheten anser dock inte att det föreslagna undantaget för luftfartyg är ändamålsenligt utformat eftersom det ofta behövs snabba insatser utan att kravet på allvarlig brottslighet har uppnåtts. Polismyndigheten anser vidare att det är en praktisk omöjlighet att genom skyltning upplysa om kamerabevakning med drönare. När det gäller möjligheten att ansöka om undantag i enskilda fall menar Polismyndigheten vidare att detta innebär att tillsynsmyndigheten i praktiken ges möjlighet att styra polisens operativa arbete på ett sätt som inte är bra. *Riksdagens ombudsmän (JO)* framhåller att det nya undantaget från upplysningskravet som tar sikte på Polismyndighetens och Säkerhetspolisens användning av drönare i akuta fall innebär att det kan bli fråga om dold kameraövervakning. Enligt JO har utredningen inte närmare beskrivit vilka behov Polismyndigheten har av det föreslagna undantaget och inte heller närmare behandlat förhållandet till reglerna i lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Om dold kameraövervakning ska vara möjlig utan de rättssäkerhetsgarantier som en prövning av åklagare och domstol ger bör det enligt JO:s mening finns ett tydligt och tungt vägande behov av detta. Bestämmelser med sådan innebörd bör vidare utformas så att det inte råder någon oklarhet om vilket regelverk som ska tillämpas i en enskild situation. Dessutom bör det enligt JO övervägas om det ska ges några andra rättssäkerhetsgarantier som kan bidra till att undantaget endast tillämpas i de situationer som det är avsett för, t.ex. en skyldighet för Polismyndigheten och Säkerhetspolisen att lämna information till tillsynsmyndigheten om de tillfällen man har tillämpat undantaget. *Svenska Journalistförbundet* anser att Polismyndighetens och Säkerhetspolisens möjligheter att utan upplysningsplikt bedriva kamerabevakning med drönare bör hanteras inom ramen för regleringen om hemlig kameraövervakning. *Stockholms läns landsting* framhåller att det finns praktiska svårigheter att uppfylla kravet vid användning av drönare och ambulans och att sådan kamerabevakning inom bl.a. hälso- och sjukvård därför bör undantas från upplysningskravet. Även *Sjöräddningssällskapet* påpekar de praktiska svårigheterna att upplysa om kamerabevakning med drönare, inte minst om flygningarna sker över vatten.

Skälen för regeringens förslag

I 27 § kameraövervakningslagen finns vissa undantag från lagens upplysningsplikt. Enligt dessa undantag behöver upplysning om övervakningen inte lämnas vid 1) övervakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning, 2) övervakning som sker för att skydda vissa angivna skyddsobjekt, 3) övervakning som Försvarsmakten bedriver från fordon, fartyg eller luftfartyg som ett led i en militär insats eller övning eller som behövs för att prova utrustning för

sådan övervakning, eller 4) övervakning som bedrivs av den som är räddningsledare enligt lagen om skydd mot olyckor, om övervakningen är av vikt för att efterforska en försvunnen person. Undantagen från upplysningsplikten gäller dock inte om ljud ska avlyssnas eller tas upp vid övervakning. Om det finns synnerliga skäl får länsstyrelsen också besluta om undantag från upplysningsplikten i enskilda fall. En ansökan om undantag ska vara skriftlig och, om övervakningsutrustningen ska kunna riktas mot en arbetsplats dit allmänheten har tillträde, innehålla ett yttrande från skyddsombudet, skyddskommittén eller en organisation som företräder de anställda på den aktuella arbetsplatsen. Länsstyrelsen ska vidare förena ett beslut om undantag med de villkor som behövs.

Som utredningen konstaterar bör utgångspunkten vara att de nuvarande undantagen från upplysningsplikten i kameraövervakningslagen ska behållas i kamerabevakningslagen eftersom de skäl som en gång motiverat undantagen fortfarande gör sig gällande. Undantagen har tillkommit bl.a. med hänvisning till att integritetsintrånget i de aktuella fallen är begränsat och att själva syftet med övervakningen skulle motverkas genom ett ovillkorligt krav på upplysning (se bl.a. prop. 1989/90:119 s. 30).

För att undantagen ska få motsvarande innebörd i den nya kamerabevakningslagen som i den nuvarande regleringen behöver de dels utgöra undantag från den upplysningsplikt som ska gälla enligt lagen och dels utgöra undantag från den rätt till information om personuppgiftsbehandling som i huvudsak kommer att styras av regleringen i dataskyddsförordningen och brottsdatalagen.

EU-regleringen tillåter vissa nationella undantag från rätten till information

Som framgår av föregående avsnitt innehåller dataskyddsförordningen och det nya dataskyddsdirektivet bestämmelser om rätten för enskilda att få information om personuppgiftsbehandling från den personuppgifts-ansvarige. Denna rätt till information kan emellertid under vissa förutsättningar begränsas i den nationella lagstiftningen. Enligt artikel 23 i dataskyddsförordningen ska en sådan begränsning ske med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgöra en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa vissa närmare angivna intressen, bl.a. den nationella säkerheten, den allmänna säkerheten, förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott och andra av unionens eller en medlemsstats viktiga mål av generellt allmänt intresse. I enlighet med skäl 73 till dataskyddsförordningen innefattar begreppet allmän säkerhet bl.a. åtgärder för att skydda människoliv, särskilt vid naturkatastrofer eller katastrofer framkallade av människan.

Enligt artikel 13.3 i det nya dataskyddsdirektivet får medlemsstaterna på motsvarande sätt anta lagstiftningsåtgärder som gör att den information som i specifika fall ska lämnas till den registrerade får senareläggas, begränsas eller utelämnas, i den utsträckning och så länge som en sådan åtgärd är nödvändig och proportionell i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen. Sådana begränsningar kan enligt direktivet ske bl.a. i syfte att undvika menlig inverkan på förebyggande, förhindrande,

upptäckt, utredning eller lagföring av brott, skydda den allmänna säkerheten eller skydda den nationella säkerheten. Den allmänna information som ska göras tillgänglig för den registrerade enligt artikel 13.1 i direktivet, exempelvis den personuppgiftsansvariges identitet och kontaktuppgifter, får dock inte begränsas på motsvarande sätt. Enligt 4 kap. 5 § i förslaget till brottsdatalag gäller den rätt till personrelaterad information som föreskrivs i lagen inte i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut av hänsyn till de intressen som pekas ut i direktivet.

De nuvarande undantagen bör behållas och utvidgas

Vid kamerabevakning som bedrivs av Polismyndigheten vid automatisk hastighetsövervakning samlas uppgifter in när ett fordon har överskridit gällande hastighetsbegränsning. Uppgifterna kan sedan användas i en brottsutredning som omfattas av bestämmelserna om förundersökning i rättegångsbalken. Dessa bestämmelser innehåller bl.a. krav på att den som är skäligen misstänkt ska underrättas om misstanken och få ta del av det som har förekommit vid förundersökningen. Kamerabevakning vid hastighetsövervakning omfattas av regleringen i det nya dataskyddsdirektivet. Undantaget i kameraövervakningslagen för sådan bevakning syftar till att undvika menlig inverkan på upptäckt, utredning eller lagföring av ett särskilt brott. Mot den bakgrunden instämmer regeringen i utredningens bedömning att ett undantag av detta slag är förenligt med EU-regleringen och bör införas i kamerabevakningslagen.

Det nuvarande undantaget för kameraövervakning av vissa skyddsobjekt syftar framför allt till att skydda den nationella säkerheten. De skyddsobjekt som omfattas av det aktuella undantaget är i stor utsträckning objekt som är av betydelse för försvarets verksamhet eller är avsedda för samhällsviktiga civila ändamål, som t.ex. energiförsörjning och elektroniska kommunikationer. Det har ansetts att ett absolut upplysningskrav på ett olyckligt sätt skulle fästa uppmärksamhet på sådana betydelsefulla anläggningar och platser (se prop. 1975/76:194 s. 22). Personuppgiftsbehandling som sker i en verksamhet som avser nationell säkerhet faller utanför EU-regleringens tillämpningsområde och kan därför regleras friare i svensk rätt. Det aktuella undantaget bör mot denna bakgrund behållas. Vidare bör undantaget utvidgas så att det motsvarar den utvidgning av undantaget från tillståndskravet som föreslås i avsnitt 6.5. Det innebär att även sådana skyddsobjekt som används för eller är avsedda för fredstida krishantering enligt 4 § 4 skyddslagen samt sådana skyddsobjekt som avses i 5 § 5 skyddslagen bör få kamerabevakas utan att upplysning eller information behöver lämnas.

Kameraövervakningslagens nuvarande undantag från upplysningsplikten för viss övervakning som bedrivs av Försvarsmakten från fordon, fartyg eller luftfartyg har motiverats dels av att uppgifter om sådan övervakning ofta omfattas av försvarssekretess och dels av att det sällan är praktiskt möjligt att upplysa om sådan övervakning (prop. 2012/13:115 s. 55). Dessa skäl gör sig fortfarande gällande och det är angeläget att sådan kamerabevakning som bedrivs av Försvarsmakten inte försvåras med anledning av den nya regleringen. Försvarsmaktens

verksamhet faller i regel utanför EU-regleringens tillämpningsområde och det aktuella undantaget måste under alla förhållanden anses som en nödvändig åtgärd i syfte att skydda nationell säkerhet. Undantaget kan därför behållas. Av samma skäl som anförs i avsnitt 6.5 saknas anledning att, som *Försvarsmakten* föreslår, göra undantaget teknikneutralt.

Slutligen innehåller kameraövervakningslagen ett undantag från upplysningsplikten för den som är räddningsledare enligt lagen om skydd mot olyckor, om övervakningen är av vikt för att efterforska försvunna personer. Undantaget har tillkommit mot bakgrund av den skyndsamhet som måste iakttas vid sådana insatser och de svårigheter som finns att på ett verksamt sätt upplysa om övervakningen (prop. 2012/13:115 s. 57). Även om sådan övervakning ofta behöver täcka större geografiska områden är integritetsriskerna begränsade eftersom det normalt handlar om övervakning vid enstaka tillfällen av områden där få människor vistas. Eftersom kamerabevakningslagen har ett snävare tillämpningsområde än den nuvarande lagen kommer viss användning av exempelvis kamerautrustade drönare i samband med insatser av det aktuella slaget inte längre att omfattas av regleringen. Det är samtidigt angeläget att inte försämra förutsättningarna för att använda kameror som hjälpmedel vid efterforskandet av försvunna personer, i den utsträckning lagen är tillämplig. Regeringen bedömer därför i likhet med utredningen att ett undantag för sådan kamerabevakning är förenligt med EU-regleringen och bör införas i kamerabevakningslagen.

Ett nytt undantag för Polismyndighetens och Säkerhetspolisens användning av drönare

I avsnitt 6.5 föreslås att det tillfälliga undantag från tillståndskravet som gäller för Polismyndigheten och Säkerhetspolisen ska behållas och utvidgas i kamerabevakningslagen. Sådan kamerabevakning är inte undantagen från upplysningskravet i den nuvarande lagen.

Frågan om Polismyndighetens möjlighet att använda kameror utan att upplysa om det har behandlats i tidigare lagstiftningsärenden (se bl.a. propositionen Lag om allmän kameraövervakning, prop. 1997/98:64 s 25). I samband med införandet av kameraövervakningslagen uttalade den dåvarande regeringen att det inte fanns skäl att inom ramen för kameraövervakningslagstiftningen införa en utvidgad möjlighet för de brottsbekämpande myndigheterna att använda dold övervakning utan prövning i det enskilda fallet (se prop. 2012/13:115 s. 90–91).

Som bland annat *JO* framhåller är det angeläget att en klar gräns kan dras mot sådan hemlig kameraövervakning som regleras i 27 kap. rättegångsbalken och lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Enligt 27 kap. rättegångsbalken får hemlig kameraövervakning användas vid förundersökning om vissa särskilt angivna allvarliga brott. Som huvudregel krävs att någon är skäligen misstänkt för brottet och att åtgärden är av synnerlig vikt för utredningen. Den hemliga kameraövervakningen får då avse en sådan plats där den misstänkte kan antas komma att uppehålla sig. Om det inte finns någon som är skäligen misstänkt för brottet får hemlig kameraövervakning även användas för att övervaka den plats där brottet har begåtts eller en nära omgivning till denna plats, om åtgärden är av synnerlig vikt för

utredningen och syftet är att fastställa vem som skäligen kan misstänkas för brottet.

Enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott får sådan hemlig kameraövervakning som regleras i 27 kap. rättegångsbalken också användas bland annat när det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva viss angiven brottslig verksamhet. Det gäller bland annat sabotage, mordbrand, allmänfarlig ödeläggelse, uppror och terroristbrott. Åtgärden ska vara av synnerlig vikt för att förhindra den brottsliga verksamheten och skälen för åtgärden måste uppväga det intrång eller men i övrigt som åtgärden innebär för den berörde eller för något annat motstående intresse.

Allmän domstol prövar om hemlig kameraövervakning ska få ske. Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen får dock en åklagare besluta om övervakning i avvaktan på domstolens beslut. Förfarandet vid hemlig kameraövervakning är därmed kringgärdat av vissa rättssäkerhetsgarantier som inte har några motsvarigheter i kameraövervakningslagen.

Utredningen bedömer att det finns ett starkt behov för Polismyndigheten och Säkerhetspolisen att i vissa specifika fall bedriva öppen kamerabevakning i enlighet med kamerabevakningslagen, utan att upplysa om bevakningen genom skyltning eller på något annat verksamt sätt. Den kamerabevakning som avses är främst sådan bevakning i akuta situationer med risk för allvarlig brottslighet som är undantagen från tillståndskravet i lagen. I sådana situationer kan förhållandena vara sådana att det inte är praktiskt möjligt att direkt uppfylla kravet på upplysning. Exempel på situationer av detta slag är våldsamma sammandrabbningar på offentliga platser, terrorangrepp eller andra plötsliga händelser som innefattar en risk för allvarlig brottslighet. När bevakning av sådana händelser ska ske från drönare eller annars från luften, dvs. med luftfartyg, är det ofta inte möjligt att upplysa om kameraanvändningen. Till skillnad mot hemlig kameraövervakning där själva poängen med övervakningen är att den sker dolt handlar det alltså om fall där kamerabevakning sker på ett öppet sätt men där de praktiska möjligheterna att upplysa om bevakningen är mycket små. Regeringen delar utredningens bedömning att det finns skäl att införa ett undantag från upplysningskravet som tar sikte på sådana situationer. Ett sådant undantag måste dock avgränsas noggrant och utformas så att det inte innebär ett kringgående av regleringen om hemlig kameraövervakning.

Behov av undantag från kravet på upplysning finns typiskt sett inte när bevakningen ska ske från rörliga objekt på marken, t.ex. fordon, eftersom en synlig upplysning kan lämnas på objektet, exempelvis genom en klisterlapp. Något sådant behov finns inte heller vid kamerabevakning från fasta objekt som avser en avgränsad geografisk plats. Vidare bör ett undantag från upplysningskravet avgränsas så att det endast gäller situationer som är brådskande. I situationer som inte är brådskande går det oftast att uppfylla kravet på upplysning även vid användning av en kamerautrustad drönare, i vart fall om bevakningen huvudsakligen ska ske inom en avgränsad plats.

Ett strikt begränsat undantag av det aktuella slaget får anses förenligt med regleringen i det nya dataskyddsdirektivet. Direktivet innebär i och för sig ett krav på att viss allmän information alltid ska göras tillgänglig

för registrerade (artikel 13.1). Det handlar bl.a. om den personuppgiftsansvariges identitet och kontaktuppgifter, ändamålen med behandlingen och rätten att lämna in klagomål till tillsynsmyndigheten. Hur sådan allmän information ska göras tillgänglig för en obestämd krets måste avgöras genom en tillämpning av aktuella bestämmelser i brottsdatalagen (4 kap. 1 §). Av skäl 42 till det nya dataskyddsdirektivet framgår emellertid att sådan information kan anges på myndighetens webbplats.

Regeringen anser, till skillnad från *Polismyndigheten*, att undantaget endast bör omfatta situationer då det av särskild anledning finns risk för allvarlig brottslighet. En mer generell utformning av undantaget skulle sträcka sig betydligt längre än motsvarande tillfälliga undantag från tillståndskravet och vara svårt att överblicka konsekvenserna av. Det bör dock framhållas att det inte krävs en misstanke om ett visst konkret brott för att undantaget ska vara tillämpligt. Det räcker att det av särskild anledning finns risk för allvarlig brottslighet. Undantaget bör dessutom utvidgas på samma sätt som motsvarande tillfälliga undantag från tillståndskravet och således omfatta alla former av allvarlig brottslighet. Det bör, till skillnad mot utredningens förslag, inte heller krävas att risken för allvarlig brottslighet kan knytas till en viss plats.

Även om det oftare är svårare att upplysa om kamerabevakning med drönare än vid annan kamerabevakning bör det som framhålls ovan normalt finnas möjligheter att genom skyltning eller på annat verksamt sätt upplysa om att bevakningen när situationen inte är brådskande. Som föreslås nedan bör det dessutom även fortsättningsvis finnas en möjlighet att ansöka om undantag från upplysningskravet hos tillsynsmyndigheten i enskilda fall.

Mot bakgrund av vad bl.a. *JO* anför om riskerna för ökad dold kamerabevakning vill regeringen framhålla att även den nuvarande kameraövervakningslagen innehåller vissa undantag från huvudregeln om upplysningsplikt som inte har ansetts innebära ett kringgående av regleringen om hemlig kameraövervakning. De särskilda undantagen i lagen tar i och för sig inte direkt sikte på brottsbekämpande myndigheters övervakning men den möjlighet som finns för länsstyrelsen att besluta om undantag i enskilda fall har inte begränsats i detta avseende (jfr prop. 2012/13:115 s. 90). Regeringen vill också framhålla att undantaget inte är avsett att omfatta fall som avses i regleringen om hemlig kameraövervakning. Undantaget innefattar således inte en rätt att försöka dölja kamerabevakningen eller att använda den som ett led i en pågående förundersökning. I kravet på att undantaget bara får tillämpas i brådskande fall ligger också att upplysning om kamerabevakningen ska lämnas när det är möjligt.

Av förslaget till brottsdatalag framgår bl.a. att tillsynsmyndigheten har rätt att från den som är personuppgiftsansvarig få upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder liksom ett antal befogenheter att förebygga och korrigera olaglig personuppgiftsbehandling (5 kap. 5–7 §§). Regeringen anser därför inte att det finns behov av att införa en särskild skyldighet för berörda myndigheter att lämna information till tillsynsmyndigheten när man har tillämpat undantaget.

Sammanfattningsvis bör ett begränsat undantag från upplysningskravet och rätten till information för den registrerade gälla vid sådan

kamerabevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller Säkerhetspolisen, om det av särskild anledning finns risk för allvarlig brottslighet och syftet med bevakningen är att förebygga, förhindra eller upptäcka sådan brottslig verksamhet eller utreda eller lagföra sådana brott.

Nytt undantag för drönare vid olyckor

I avsnitt 6.6 föreslås att kamerabevakningslagen ska innehålla ett undantag från tillståndskravet för viss kamerabevakning som bedrivs i samband med olyckor av Polismyndigheten eller den som är räddningsledare enligt lagen om skydd mot olyckor. Undantaget motsvaras i allt väsentligt av det nuvarande tillfälliga undantaget i 11 § första stycket 1 kameraövervakningslagen och är främst avsett att komma till användning i anslutning till att avspärrning har skett på grund av en olycka, en katastrof eller någon annan nödfallsliknande situation (se prop. 1997/98:64 s. 56 och 2012/13:115 s. 56). Kameraövervakningslagen innehåller inte något undantag från upplysningskravet vid sådan kameraövervakning.

Frågan är om det finns ett behov av ett undantag även från upplysningsplikten vid kamerabevakning som behövs vid hotande eller inträffade olyckor. Det kan konstateras att det i sådana situationer i regel finns behov av att snabbt kunna få en överblick av olycksområdet och att kamerautrustade drönare eller andra luftfartyg kan utgöra användbara hjälpmedel för att få en sådan överblick. Visserligen kommer sådan användning av kameror ofta inte att omfattas av den nya lagens tillämpningsområde eftersom det normalt inte är fråga om vare sig varaktig eller regelbundet upprepad personbevakning. I de fall där kamerabevakningslagen är tillämplig kan det dock, åtminstone inledningsvis, vara svårt eller praktiskt omöjligt att uppfylla upplysningskravet på grund av det olycksdrabbade områdets storlek och behovet av skyndsamhet.

I dessa fall måste integritetsriskerna anses små i förhållande till intresset av kamerabevakningen. Intresset av att rädda människoliv, särskilt vid naturkatastrofer eller katastrofer framkallade av människan, anges i skäl 73 till dataskyddsförordningen som ett exempel på när en begränsning av förordningens rättigheter kan göras enligt artikel 23. De människor som råkar befinna sig i ett olycksområde får åtminstone inledningsvis anses ha ett begränsat intresse av att bli upplysta om kamerabevakningen. Om bevakningen behövs även efter det akuta inledningsskedet bör det dessutom oftast vara möjligt att uppfylla kravet på upplysning och information. I den mån även detta av praktiska skäl är omöjligt kan undantag beviljas i enskilda fall.

Regeringen instämmer mot denna bakgrund i utredningens bedömning att det bör införas ett undantag från upplysningsplikten vid kamerabevakning vid olyckor. Som *MSB* anför bör det framgå att undantaget även omfattar kamerabevakning i samband med efterföljande åtgärder vid risk för nya olyckor, under förutsättning att det rör sig om kamerabevakning i brådskande fall och upplysning därför inte kan lämnas. Att ge undantaget en mer generell utformning skulle emellertid kunna innebära att det omfattar fler fall än vad som är strikt nödvändigt.

Mot denna bakgrund bör ett undantag från upplysningskravet och rätten till information för den enskilde gälla vid sådan kamerabevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller den som är räddningsledare enligt lagen om skydd mot olyckor, om bevakningen är av vikt för att avvärja en överhängande fara för olycka, begränsa verkningarna av en inträffad olycka eller minska risken för nya olyckor.

Undantag ska också kunna beslutas i enskilda fall

Bestämmelsen i 27 § tredje stycket kameraövervakningslagen om att undantag från upplysningsplikten kan göras i enskilda fall om det finns synnerliga skäl är avsedd att tillämpas restriktivt. I förarbetena har som exempel angetts övervakning av rovdjurslyor i syfte att upptäcka och beivra tjuvskytte och plundring samt för att kartlägga rovdjurens bestånd (se prop. 2012/13:115 s. 89–91). Det har alltså ansetts viktigt att kunna bedriva kamerabevakning för viltvårds- och artskyddsändamål utan att t.ex. rovdjurslyors lägen avslöjas eftersom syftet med bevakningen då motverkas. I förarbetena har också uttalats att det kan förekomma angelägna behov av undantag även i andra fall. Det kan t.ex. röra sig om fall där det inte är möjligt att på ett verkningsfullt sätt upplysa om övervakningen.

Den tekniska utvecklingen av bl.a. kamerautrustade drönare innebär att det allt oftare kan uppstå situationer där det är angeläget att kunna använda tekniken men praktiskt omöjligt att fullt ut uppfylla upplysningskravet. I viss utsträckning undviks sådan problematik genom att kamerabevakningslagen får ett snävare tillämpningsområde än den nuvarande lagstiftningen. Den som vill använda kamerautrustade drönare i andra syften än att bevaka människor bör ofta kunna se till att användningen inte innebär varaktig eller regelbundet upprepad personbevakning. Därmed gäller inte upplysningskravet i kamerabevakningslagen. Enligt regeringens bedömning bör t.ex. användning av kamerautrustade drönare i sådana verksamheter som *Sjöräddningssällskapet* och *Stockholms läns landsting* uppmärksammar ofta falla utanför lagens tillämpningsområde. Detsamma gäller räddningsverksamhet som bedrivs av frivilligorganisationer.

Som utredningen föreslår bör det dessutom även fortsättningsvis finnas möjligheter för tillsynsmyndigheten att i enskilda fall besluta om undantag från kravet på upplysning och information om den personuppgiftsbehandling som kamerabevakningen innebär. Detta säkerställer att lagstiftningen inte hindrar särskilt angelägen användning av kameratekniken, exempelvis i sjukvårds- och räddningsverksamhet. Prövningen bör precis som i dag präglas av restriktivitet genom att ett krav på synnerliga skäl ställs upp. Den tekniska utvecklingen, t.ex. i fråga om kamerautrustade drönare, innebär emellertid att det kan finnas anledning att besluta om undantag i fler fall än tidigare, om detta är en förutsättning för att tekniken ska kunna användas i angelägna fall.

Utöver de nämnda fallen bör undantag exempelvis kunna komma i fråga vid Polismyndighetens användning av drönare i andra situationer än sådana brådskande fall som det särskilda undantaget tar sikte på. Ett sådant exempel är användningen av kamerautrustade drönare i samband med

förväntade oroligheter vid exempelvis statsbesök eller andra planerade evenemang där bevakningen framstår som angelägen men sannolikt inte kan begränsas till ett visst område och upplysningskravet i praktiken därför inte går att uppfylla. I sammanhanget kan också framhållas att en ansökan om undantag från upplysningskravet kan ske redan i samband med en ansökan om tillstånd till kamerabevakning om det skulle vara aktuellt. En och samma ansökan bör vidare, precis som vid tillståndsförfarandet, kunna omfatta kamerabevakning från flera olika drönare (se avsnitt 6.4).

Regeringen bedömer, i likhet med utredningen, att en sådan lagreglerad och begränsad möjlighet till beslut om undantag i enskilda fall som nu föreslås är förenlig med EU-regleringen.

Förfarandet vid tillsynsmyndighetens beslut om undantag i enskilda fall

Kamerabevakningslagen behöver liksom den nuvarande regleringen innehålla bestämmelser om förfarandet vid tillsynsmyndighetens beslut om undantag i enskilda fall.

Enligt 27 § tredje stycket kameraövervakningslagen ska en ansökan om undantag från upplysningsplikten vara skriftlig. Vidare ska ett yttrande från skyddsombudet, skyddskommittén eller en organisation som företräder de anställda på arbetsplatsen lämnas in tillsammans med ansökan och berörd kommun ges tillfälle att yttra sig i vissa fall. Ett beslut om undantag ska förenas med de villkor som behövs, t.ex. under vilken tid undantaget gäller. Om förutsättningarna för ett beslut om undantag ändras får, enligt 20 § kameraövervakningslagen, nya villkor beslutas eller, om förutsättningarna för tillstånd inte längre uppfylls, beslutet återkallas.

Kamerabevakningslagen bör innehålla motsvarande bestämmelser om förfarandet. I enlighet med utredningens förslag bör det i kamerabevakningslagen på ett utförligare sätt än tidigare anges vilka uppgifter en ansökan ska innehålla. Dessutom bör det framgå att berörd kommun, precis som vid tillståndsprövningen, bara ska ges tillfälle att yttra sig om det av särskild anledning behövs ett yttrande. Ett beslut om undantag bör, precis som ett tillståndsbeslut, få begränsas att gälla en viss tid.

Undantag för avlyssning eller inspelning av ljud

Kamerabevakning som innefattar avlyssning och upptagning av ljud innebär i regel särskilt påtagliga integritetsrisker eftersom det normalt inte finns anledning att förvänta sig att utomstående ska ta del av vad man säger även om man befinner sig i en offentlig miljö. Detta är en viktig utgångspunkt även för den nya lagen.

Varken kameraövervakningslagens generella undantag från upplysningsplikten eller möjligheten till beslut om undantag i enskilda fall gäller om ljud ska avlyssnas eller tas upp vid övervakningen. Enligt utredningen har det dock framkommit att det försvårar bevakning som sker för att kartlägga bestånd av hotade rovdjur. Vid sådana kartläggningar görs bl.a. undersökningar av föryngringen av rovdjursstammen och en möjlighet att registrera ljudet från rovdjursungarna är då ofta en förutsättning för att en bedömning av föryngringen ska vara möjlig. Enligt *MSB* kan det också vara värdefullt för räddningstjänsten att i vissa fall kunna uppfatta ljud som exempelvis ras, explosion eller rop på hjälp.

Regeringen delar utredningens bedömning att de särskilda undantagen inte heller fortsättningsvis bör innefatta en rätt att utan upplysning avlyssna eller spela in ljud. Däremot bör det i enlighet med vad utredningen föreslår finnas möjlighet att efter noggranna överväganden också undanta sådan kamerabevakning från upplysningskravet i enskilda fall. En förutsättning för detta bör vara att intresset av avlyssning eller upptagning av ljud väger tungt samtidigt som integritetsriskerna i praktiken är obefintliga. Utöver de exempel som anges ovan kan så t.ex. vara fallet vid Polismyndighetens användning av sensorer som kan detektera ljud av skottlossning eller liknande. Undantaget får dock inte tillämpas på ett sätt som möjliggör hemlig eller dold avlyssning av människors samtal.

8 Ett förstärkt integritetsskydd vid kamerabevakning på arbetsplatser

Regeringens förslag: Kamerabevakningslagen ska innehålla en bestämmelse som upplyser om att det i fråga om arbetsgivares kamerabevakning av en arbetsplats finns bestämmelser om förhandlingsskyldighet i 11–14 §§ lagen (1976:580) om medbestämmande i arbetslivet.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår en bestämmelse som innebär en materiell reglering av förhandlingsskyldigheten enligt lagen om medbestämmande i arbetslivet (MBL) vid kamerabevakning på arbetsplatser som inte omfattas av kravet på tillstånd. Utredningen föreslår också en bestämmelse om att undantag från förhandlingsskyldigheten ska få göras genom kollektivavtal.

Remissinstanserna: En majoritet av remissinstanserna, däribland *Datainspektionen*, *Arbetsmiljöverket* och *Statens Skolinspektion*, tillstyrker eller har inga synpunkter på förslaget. Även *Arbetsdomstolen* tillstyrker förslaget i sig men anser att det bör övervägas om det också bör införas en materiell hänvisning till de skadeståndssanktionerade bestämmelserna i 15–18, 21 och 22 §§ MBL om hur det ska gå till vid förhandlingen. Enligt Arbetsdomstolen framstår det vidare som en brist i förslaget att den berörda arbetstagarorganisationen inte kan utkräva någon sanktion, om inte underlåtenheten att förhandla samtidigt innebär ett brott mot lagen om medbestämmande i arbetslivet eller kollektivavtal. Arbetsdomstolen föreslår därför att lagförslaget kompletteras med en reglering om att skadestånd kan utgå till berörd arbetstagarorganisationen om arbetsgivaren inte fullföljer sin förhandlingsskyldighet enligt kamerabevakningslagen. Enligt Arbetsdomstolen bör också den reglering om preskription som följer av MBL gälla. *Landsorganisationen i Sverige (LO)* välkomnar att det föreslås en anpassning till den svenska partsmodellen även om LO och medlemsförbunden anser att det gäller en förhandlingsskyldighet för arbetsgivare även enligt det nuvarande

rättsläget. Den bristande tillämpningen beror enligt LO:s uppfattning ofta på bristande kunskap om regelverket. Även *Sveriges Akademikers Centralorganisation (Saco)* anser att beslut om kamerabevakning på en arbetsplats redan i dag som regel omfattas av förhandlingsskyldigheten i lagen om medbestämmande i arbetslivet. Saco tycker dock att det är bra att detta förtydligas eftersom det är osäkert om regleringen efterlevs. *Tjänstemännens Centralorganisation (TCO)* tillstyrker förslaget om förhandlingsskyldighet men anser samtidigt att det bör klargöras i vad mån bestämmelsen i kamerabevakningslagen har någon materiell betydelse när förhandlingsskyldighet samtidigt föreligger enligt lagen om medbestämmande i arbetslivet, eller om den då enbart har en upplysningsfunktion. TCO ställer sig också frågande till innebörden av den föreslagna undantagsbestämmelsen och vad den kan leda till arbetsrättsligt. *Svensk Handel* och *Svenskt Näringsliv* avstyrker förslaget med hänvisning till det förstärkta integritetsskydd som dataskyddsförordningen innebär och olämpligheten av att införa ett absolut krav på förhandlingsskyldighet i en särskild lag. *Arbetsgivarverket* och *Visita* framför liknande synpunkter men öppnar i och för sig upp för någon form av upplysningsbestämmelse som, i likhet med viss annan lagstiftning på arbetsrättens område, hänvisar till regleringen i lagen om medbestämmande i arbetslivet.

Skälen för regeringens förslag

Nuvarande integritetsskydd och behovet av förstärkning

Kamerabevakning av arbetsplatser är mycket vanligt förekommande i vissa branscher och kan samtidigt medföra särskilda risker för de anställdas personliga integritet. Många anställda måste vistas regelbundet på platser som kamerabevakas av arbetsgivaren och kan samtidigt känna olust inför att invända mot kamerabevakningen eller påtala brister på grund av det särskilda beroendeförhållande som anställningsförhållandet innebär.

Enligt kameraövervakningslagen krävs som huvudregel tillstånd till kameraövervakning av platser dit allmänheten har tillträde. Om övervakningen avser en arbetsplats ska ett yttrande från skyddsombudet, skyddskommittén eller en organisation som företräder de anställda på arbetsplatsen lämnas in tillsammans med ansökan. Denna reglering ger enligt regeringens bedömning ett tillfredsställande skydd för den personliga integriteten vid kameraövervakning av sådana arbetsplatser. Även enligt kamerabevakningslagen kommer det att finnas ett krav på att yttrande från skyddsombudet, skyddskommittén eller en organisation som företräder de anställda på arbetsplatsen ska lämnas in tillsammans med en ansökan om tillstånd till kamerabevakning, eller en ansökan om undantag från upplysningskravet (se avsnitt 6.4 och 7.2). Samtidigt innebär förslaget att tillståndsplikten inte kommer att omfatta privata arbetsgivare, om de inte utför en uppgift av allmänt intresse. Det finns därför skäl att överväga åtgärder för att säkerställa integritetsskyddet vid kamerabevakning på sådana arbetsplatser.

Det har vidare framkommit att det finns brister i tillämpningen av den nuvarande lagen vid kameraövervakning av utrymmen på arbetsplatser dit allmänheten inte har tillträde. När det gäller kameraövervakning av sådana

platser finns det i kameraövervakningslagen inte något krav på yttrande eller överenskommelse med skyddsombud, skyddskommitté eller en organisation som företräder de anställda på arbetsplatsen. Enligt Integritetskommittén har tillsynsmyndigheterna bl.a. uppmärksammat fall där informationen till de anställda är bristfällig eller obefintlig, där övervakningen felaktigt grundar sig på anställdas samtycke och där inspelat material används för att kontrollera hur de anställda arbetar (se SOU 2016:41 s. 232–234). Det finns därför skäl att överväga om skyddet för den personliga integriteten bör förstärkas på arbetsplatser.

Förhandlingsskyldighet vid kamerabevakning av arbetsplatser

Enligt 11 § MBL ska en arbetsgivare innan denne beslutar om en viktigare förändring av sin verksamhet på eget initiativ förhandla med en arbetstagarorganisation i förhållande till vilken arbetsgivaren är bunden av kollektivavtal. Detsamma ska iakttas innan en arbetsgivare beslutar om en viktigare förändring av arbets- eller anställningsförhållandena för arbetstagare som tillhör organisationen. Om synnerliga skäl föranleder det får arbetsgivaren dock fatta och verkställa beslut innan han eller hon har fullgjort denna förhandlingsskyldighet.

Även i annat fall ska enligt 12 § MBL en arbetsgivare förhandla med kollektivavtalsbärande arbetstagarorganisation innan han eller hon fattar eller verkställer beslut som rör en medlem i denna, om organisationen påkallar detta. Om särskilda skäl föranleder det får arbetsgivaren dock fatta och verkställa beslutet innan han eller hon har fullgjort denna förhandlingsskyldighet. Av 13 § MBL följer att en arbetsgivare på motsvarande sätt kan vara skyldig att förhandla med en arbetstagarorganisation i förhållande till vilken arbetsgivaren inte är bunden av kollektivavtal. I enlighet med 14 § MBL ska förhandlingsskyldigheten enligt 11–13 §§ i första hand fullgöras genom förhandling med en lokal arbetstagarorganisation förutsatt att en sådan finns. Om enighet vid förhandlingen inte uppnås ska arbetsgivaren på begäran förhandla även med en central arbetstagarorganisation.

Frågor som rör ett förstärkt integritetsskydd i arbetslivet har utretts flera gånger utan att det har lett till lagstiftning. Integritetsutredningen (N 1999:10) föreslog i sitt betänkande Personlig integritet i arbetslivet (SOU 2002:18) en särskild lag om skydd för personlig integritet i arbetslivet. Enligt förslaget skulle lagen bl.a. innehålla en bestämmelse som upplyser om att 11–14 §§ MBL gäller i fråga om arbetsgivarens skyldighet att förhandla före beslut som rör verksamheten. Syftet med förslaget var att framhäva vikten av att arbetstagarnas inflytande uppmärksammas i frågor som innefattar integritet i arbetslivet. Utredningen om integritetsskydd i arbetslivet (N 2006:07) föreslog i sitt betänkande Integritetsskydd i arbetslivet (SOU 2009:44) en särskild lag om integritet i arbetslivet. Förslaget innehåller bl.a. en bestämmelse om att en arbetsgivare som avser att besluta om en övervaknings- eller kontrollåtgärd som är ägnad att på ett påtagligt sätt påverka en eller flera arbetstagares personliga integritet först ska förhandla med berörd arbetstagarorganisation på det sätt som anges i 11–14 §§ MBL.

Det behövs en upplysningsbestämmelse

Visserligen medför dataskyddsförordningen, som bl.a. *Svensk Handel* och *Svenskt Näringsliv* framhåller, en förstärkning av integritetsskyddet för arbetstagare. Regeringen anser emellertid inte att denna generella förstärkning av integritetsskyddet är tillräcklig med tanke på de brister som har uppmärksammats i tillämpningen av den nuvarande regleringen. Det är därför angeläget att den nya lagen leder till ett förstärkt integritetsskydd vid kamerabevakning på arbetsplatser. Regeringen anser att detta bör ske genom att det i kamerabevakningslagen införs en hänvisning till reglerna i lagen om medbestämmande i arbetslivet, en uppfattning som delas av bl.a. *Datainspektionen.*

En hänvisning till regleringen i lagen om medbestämmande i arbetslivet kan utformas på två sätt, antingen som en materiell bestämmelse som syftar till att reglera en förhandlingsskyldighet eller som en upplysningsbestämmelse. Utredningen föreslår en bestämmelse som innebär en materiell reglering av förhandlingsskyldigheten som gäller vid kamerabevakning på arbetsplatser som inte omfattas av kravet på tillstånd. Som flera remissinstanser påtalar, däribland *Landsorganisationen i Sverige (LO*) och *Sveriges Akademikers Centralorganisation (Saco),* innebär emellertid regleringen i 11–14 §§ MBL att en förhandlingsskyldighet för arbetsgivare i de allra flesta fall redan föreligger inför kamerabevakning av arbetsplatser.

Vidare finns det, som bland andra *Arbetsgivarverket* påpekar, fördelar med en bestämmelse av upplysningskaraktär. En sådan ordning stämmer för det första bättre överens med övrig arbetsrättslig reglering. För det andra blir det också tydligt att det är den materiella regleringen i lagen om medbestämmande i arbetslivet som gäller fullt ut också i övrigt. Exempelvis bör frågor om hur förhandlingen ska gå till, rätten till information, skadestånd, preskription och sanktioner styras av den arbetsrättsliga regleringen och inte av regleringen i dataskyddsförordningen. Det skulle därmed inte finnas något behov av någon sådan ytterligare reglering i kamerabevakningslagen som *Arbetsdomstolen* efterfrågar. En upplysningsbestämmelse skulle också råda bot på den okunskap om regelverket som *LO* pekar ut som den främsta orsaken till de brister i tillämpningen som konstaterats.

Enligt regeringens uppfattning måste förhandlingsskyldigheten i 11 § MBL normalt anses gälla inför arbetsgivares beslut om kamerabevakning som innebär att anställda varaktigt eller regelbundet bevakas. Dessutom har arbetstagarorganisationerna en möjlighet att påkalla förhandling på eget initiativ enligt 12 § MBL. En upplysningsbestämmelse av det aktuella slaget kan till skillnad mot utredningens förslag också omfatta kamerabevakning på arbetsplatser generellt.

Regeringen anser sammanfattningsvis att kamerabevakningslagen bör innehålla en bestämmelse som upplyser om att det i fråga om arbetsgivares kamerabevakning av en arbetsplats finns bestämmelser om förhandlingsskyldighet i 11–14 §§ MBL.

9 Ett förstärkt integritetsskydd i övrigt

Regeringens bedömning: Integritetsskyddet vid kamerabevakning förstärks genom att regleringen i EU:s dataskyddsförordning, dataskyddslagen och brottsdatalagen kommer att gälla i tillämpliga delar. Kamerabevakningslagen bör därför inte innehålla särskilda bestämmelser om allmänna principer för behandling av personuppgifter, lagringstid, rättigheter för enskilda, skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden eller överföring av personuppgifter till tredjeland eller internationella organisationer.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: En majoritet av remissinstanserna instämmer i eller har inga invändningar mot bedömningen. *Datainspektionen* ifrågasätter utredningens bedömning att kamerabevakarens intresse alltid väger tyngre så länge bevakningen håller sig inom villkoren för ett meddelat tillstånd. *Domstolsverket* anser att en särskild bestämmelse om bevarandetid bör övervägas eftersom det finns en risk för att bildmaterial annars kan komma att bevaras längre tid än nödvändigt. *Svenskt näringsliv* efterfrågar en EU-harmoniserad tolkning av artikel 10 i dataskyddsförordningen och därigenom utvidgade möjligheter till kamerabevakning som avser misstankar om brott.

Skälen för regeringens bedömning

Den nya dataskyddsregleringen innebär ett förstärkt integritetsskydd

Kameraövervakningslagen gäller enligt 6 § i stället för personuppgiftslagen och innehåller vissa bestämmelser som motsvarar regleringen i den sistnämnda lagen. Kameraövervakningslagen innehåller således bestämmelser om t.ex. vidarebehandling (28 §), säkerhet (30 och 31 §§), bevarande av material (32 och 33 §§) och överföring av bild- och ljudmaterial till tredjeland (34–36 §§).

Som konstateras i avsnitt 5.2.1 bör kamerabevakningslagen i princip inte innehålla bestämmelser som enbart upprepar bestämmelserna i dataskyddsförordningen. Lagen kan inte heller innehålla regler som avviker från regleringen i dataskyddsförordningen i större utsträckning än vad förordningen medger. De bestämmelser som tas in i lagen måste vidare uppfylla kraven i det nya dataskyddsdirektivet. Lagen innehåller därför endast de bestämmelser som särskilt behövs för kamerabevakning på grund av de specifika förhållanden som gäller för sådan bevakning. Kamerabevakningslagen kommer således, till skillnad från den nuvarande lagen, inte att gälla i stället för övrig dataskyddsreglering. Detta innebär att den personuppgiftsbehandling som kamerabevakning innebär till största delen kommer att regleras direkt i den tillämpliga generella dataskyddsregleringen.

Dataskyddsförordningen kommer således inom sitt tillämpningsområde att gälla för den personuppgiftsbehandling som kamerabevakningen innebär. På samma sätt kommer brottsdatalagens generella bestämmelser att gälla för kamerabevakning som innebär sådan personuppgiftsbehandling som avses i det nya dataskyddsdirektivet. Även

bestämmelser i registerförfattningar som kan tillämpas vid kamerabevakning kommer kunna bli tillämpliga. Kamerabevakning i sådan verksamhet som inte omfattas av dataskyddsförordningen eller det nya dataskyddsdirektivet, t.ex. verksamhet som avser nationell säkerhet, kommer också styras av den generella regleringen i dataskyddsförordningen om inte annat särskilt föreskrivs. Enligt förslaget till dataskyddslag ska nämligen dataskyddsförordningen och dataskyddslagen, med vissa undantag, gälla i tillämpliga delar även för personuppgiftsbehandling i sådan verksamhet (1 kap. 2 §).

Genom att den nya dataskyddsregleringen blir tillämplig förstärks t.ex. enskildas rätt till information om hur personuppgifter behandlas. Det ställs vidare strängare krav på den som behandlar personuppgifter, exempelvis genom att krav på inbyggt dataskydd och dataskydd som standard kommer att gälla. Tillsynsmyndigheten ges samtidigt ökade befogenheter och kan bl.a. besluta om sanktionsavgifter för den som bryter mot reglerna. Att låta regleringen i dataskyddsförordningen med kompletterande nationell reglering och den generella nationella regleringen som genomför det nya dataskyddsdirektivet gälla också vid kamerabevakning innebär därför en förstärkning av integritetsskyddet.

Mot bakgrund av vad *Svenskt näringsliv* framför om behovet av utvidgade möjligheter till kamerabevakning som avser misstankar om brott bör framhållas att regleringen i artikel 10 dataskyddsförordningen om behandling av personuppgifter som rör lagöverträdelser, bör tolkas så att den inte tar sikte på sådana möjliga lagöverträdelser som kan fångas på bild vid kameraövervakning (se prop. 2017/18:105 s. 98). Den aktuella bestämmelsen utgör därför i regel ingen begränsning av möjligheterna för enskilda subjekt att bedriva kamerabevakning för brottsbekämpande ändamål.

Nedan behandlas vissa bestämmelser i dataskyddsförordningen och i brottsdatalagen som är av särskild betydelse vid kamerabevakning. I samband med det övervägs om det är möjligt och lämpligt att införa avvikande bestämmelser i kamerabevakningslagen.

Inga bestämda lagringstider – allmänna principer för behandling av personuppgifter ska gälla också vid kamerabevakning

Både dataskyddsförordningen och det nya dataskyddsdirektivet innehåller allmänna principer för personuppgiftsbehandling som tillsammans med regleringen av de rättsliga grunderna utgör de grundläggande förutsättningarna för att en personuppgiftsbehandling ska vara tillåten. Bland principerna för behandling kan särskilt nämnas kraven på laglighet och korrekthet, ändamålsbegränsning, uppgiftsminimering, lagringsminimering samt integritet och konfidentialitet. Dataskyddsförordningens reglering av principer för behandling av personuppgifter i artikel 5 är direkt tillämplig medan motsvarande reglering i artikel 4 i det nya dataskyddsdirektivet kommer att genomföras genom bestämmelser brottsdatalagen.

I kameraövervakningslagen finns särskilda bestämmelser om lagringstid, vilket bl.a. *Domstolsverket* anser bör övervägas även i den nya kamerabevakningslagen. Enligt 32 § kameraövervakningslagen får bild- eller ljudmaterial från kameraövervakning av en plats dit allmänheten har

tillträde bevaras under högst två månader, om inte länsstyrelsen beslutar om en längre bevarandetid. Material från övervakning av en plats dit allmänheten inte har tillträde får inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med övervakningen. Om materialet används i någon annan verksamhet hos den som bedriver kameraövervakningen tillämpas dock i stället regleringen i personuppgiftslagen eller annan författning som gäller för behandling av personuppgifter i den verksamheten. Detta innebär exempelvis att Polismyndigheten inte är begränsad av den föreskrivna lagringstiden om materialet tas in i en förundersökning.

Några fasta tidsgränser för lagring av uppgifter finns varken i dataskyddsförordningen eller i det nya dataskyddsdirektivet. Dataskyddsförordningens princip om lagringsminimering (artikel 5.1 c) innebär dock att personuppgifter inte får 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. Motsvarande reglering finns i artikel 4.1 f i det nya dataskyddsdirektivet. I artikel 5 i direktivet anges därutöver att det ska föreskrivas lämpliga tidsgränser för radering av personuppgifter eller för periodisk översyn av behovet av att lagra personuppgifter. I brottsdatalagen föreslås därför bestämmelser om att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen och att den personuppgiftsansvarige, om inte annat är föreskrivet, årligen ska se över behovet av att fortsatt behandla personuppgifterna (2 kap. 17 och 18 §§).

Inom dataskyddsförordningens tillämpningsområde är utrymmet att införa särskilda bestämmelser om lagringstid eller på andra sätt modifiera de allmänna principerna för behandling av personuppgifter begränsade. Artikel 6.2 i förordningen ger i och för sig utrymme att införa mer specifika krav för sådan personuppgiftsbehandling som är nödvändig för att fullgöra en rättslig förpliktelse, utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Detta innebär att det skulle vara möjligt att införa särskilda bestämmelser om lagringstid för sådan kamerabevakning som omfattas av tillståndskravet.

Eftersom den tekniska utvecklingen innebär att kamerabevakning ständigt får nya användningsområden framstår det emellertid inte som ändamålsenligt att fastställa en enhetlig maximal lagringstid för upptaget material. Särskilda bestämmelser om lagringstid skulle dessutom inte kunna gälla för all kamerabevakning utan bara inom det tillståndspliktiga området. Vid sådan kamerabevakning har tillsynsmyndigheten också möjlighet att förena tillståndet med villkor om att materialet endast får lagras under en viss angiven tid. Ett sådant villkor gäller dock endast så länge materialet inte kommer till användning i någon annan verksamhet än kamerabevakning hos den som bedriver bevakningen, t.ex. Polismyndighetens användning av material från kamerabevakning i förundersökningar. I andra fall kan tillsynsmyndigheten, t.ex. i samband med konsekvensbedömningar och samråd med myndigheten, använda sig av sina tillsynsbefogenheter om den planerade bevarandetiden inte anses förenlig med den tillämpliga dataskyddsregleringen.

Mot denna bakgrund bör det inte införas några särskilda bestämmelser i kamerabevakningslagen om längsta tid för behandling av bild- och ljudmaterial från kamerabevakning. Den nya dataskyddsregleringen bedöms ge ett starkt skydd för den personliga integriteten även utan en sådan tidsgräns.

Det har inte heller framkommit skäl att införa specifika bestämmelser som rör någon av övriga allmänna principer om personuppgiftsbehandling som regleras i dataskyddsförordningen eller brottsdatalagen. Dessa principer kommer därmed att gälla även för kamerabevakning i tillämpliga delar. Det innebär bl.a. att kamerabevakning ska ske för särskilt, uttryckligt angivna och berättigade ändamål och att material från kamerabevakningen inte får sparas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

Enskildas rättigheter

Både dataskyddsförordningen och det nya dataskyddsdirektivet innehåller en rad bestämmelser om enskildas rättigheter som kan bli tillämpliga vid kamerabevakning. Enligt såväl dataskyddsförordningen (artikel 15) som förslaget till brottsdatalag (4 kap. 3 §) ska den registrerade exempelvis ha rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör honom eller henne behandlas och i så fall få tillgång till uppgifterna och viss information, bl.a. om ändamålen med behandlingen, hur länge personuppgifterna kommer att lagras, rätten till rättelse eller radering av personuppgifterna och rätten att lämna in klagomål till tillsynsmyndigheten. Någon motsvarighet till denna rättighet finns inte i kameraövervakningslagen men bör i syfte att stärka integritetsskyddet som utgångspunkt gälla också för personuppgiftsbehandling vid kamerabevakning.

Det ska samtidigt framhållas att material som lagras vid kamerabevakning i normalfallet inte är strukturerat så att det går att söka efter personuppgifter på annat sätt än manuellt. Om rätten till tillgång skulle innebära att den som bedriver kamerabevakning, på begäran av en enskild, skulle behöva gå igenom materialet och försöka identifiera den enskilde skulle regelverket riskera att skapa orimliga administrativa bördor och medföra onödiga integritetsrisker för andra personer som finns i materialet. EU-regleringen bedöms därför inte innebära att den som bedriver kamerabevakning är skyldig att vidta andra åtgärder än att utnyttja de sök- och sammanställningsmöjligheter som han eller hon har tillgång till. Även bestämmelser om sekretess och tystnadsplikt kan begränsa rätten till tillgång till material från kamerabevakning.

I såväl dataskyddsförordningen (artikel 16) som förslaget till brottsdatalag (4 kap. 9 §) finns också en rätt till rättelse av personuppgifter. Denna rättighet innebär att en registrerad utan onödigt dröjsmål ska få felaktiga personuppgifter som rör honom eller henne rättade av den personuppgiftsansvarige. Rätten innebär vidare att den registrerade, med beaktande av ändamålet med behandlingen, ska ha rätt att komplettera ofullständiga personuppgifter. Rätten till rättelse aktualiseras normalt sett inte i fråga om bild- och ljudmaterial från kamerabevakning, men skulle kunna vara tillämplig i vissa undantagssituationer, exempelvis om en felaktig tidsangivelse anges i inspelat bildmaterial. I sådana situationer

framstår det som rimligt att det finns en möjlighet att få den felaktiga informationen rättad eller kompletterad.

Dataskyddsförordningen (artikel 18–19) och förslaget till brottsdatalag (4 kap. 10 §) innehåller vidare en rätt till radering av personuppgifter och en rätt till begränsning av personuppgiftsbehandling. Även dessa rättigheter kan aktualiseras och framstå som befogade vid sådan kamerabevakning som innebär personuppgiftsbehandling. Liksom vid övrig personuppgiftsbehandling framstår det exempelvis som rimligt att enskilda har möjlighet att få material från kamerabevakning som avser honom eller henne raderat när materialet inte längre är nödvändigt för ändamålen med behandlingen.

Slutligen innehåller dataskyddsförordningen (artikel 21) en rätt för den registrerade att göra invändningar mot en behandling av personuppgifter som avser honom eller henne och som grundar sig på artikel 6.1 e eller f i förordningen. Den personuppgiftsansvarige får efter en sådan invändning inte längre behandla personuppgifterna såvida inte denne kan påvisa tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller behandlingen sker för fastställande, utövande eller försvar av rättsliga anspråk. Det nya dataskyddsdirektivet och förslaget till brottsdatalag innehåller ingen motsvarande rättighet.

Datainspektionen ifrågasätter utredningens bedömning om att intresset av kamerabevakning alltid väger tyngre än den registrerades intressen, rättigheter och friheter så länge bevakningen håller sig inom villkoren för ett meddelat tillstånd och att enskilda i sådana fall därför inte skulle ha rätt att göra invändningar. Enligt regeringens bedömning innebär ett beviljat tillstånd för kamerabevakning visserligen inte ett formellt undantag från rätten att göra invändningar. Samtidigt bör det inte vara möjligt att nå framgång med en invändning mot sådan kamerabevakning eftersom det redan genom tillståndsbeslutet konstaterats att intresset av kamerabevakning väger tyngre än den enskildes intresse av att inte bli bevakad.

Sammanfattningsvis innebär rättigheterna i dataskyddsförordningen och förslaget till brottsdatalag en förstärkning av skyddet för den personliga integriteten. Dessa rättigheter bör därför utan några särskilda begränsningar gälla i tillämpliga delar även vid kamerabevakning.

Bestämmelser om personuppgiftsansvarigas skyldigheter och om överföring av material till tredjeland

Dataskyddsförordningen innehåller en omfattande reglering om skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden. Regleringen innehåller bl.a. allmänna skyldigheter om inbyggt dataskydd och dataskydd som standard (artikel 25), säkerhet för personuppgifter (artikel 32), konsekvensbedömning (artikel 35) och förhandssamråd med tillsynsmyndigheten i vissa fall (artikel 36) samt utnämning av dataskyddsombud (artikel 37). Motsvarande bestämmelser finns också i förslaget till brottsdatalag.

Vidare innehåller kapitel V i dataskyddsförordningen reglering om under vilka förutsättningar personuppgifter får överföras till tredjeland eller till internationella organisationer. Huvudregeln är att en överföring är

tillåten, om det mottagande tredjelandet eller den mottagande organisationen kan säkerställa en adekvat skyddsnivå för uppgifterna. Även det nya dataskyddsdirektivet och förslaget till brottsdatalag innehåller bestämmelser som reglerar denna fråga.

Regleringen om skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden samt om överföring av personuppgifter till tredjeland innebär en förstärkning av skyddet för den personliga integriteten. Det finns inte skäl att i kamerabevakningslagen införa någon särskild reglering av dessa frågor.

10 Sekretess och tystnadsplikt

Regeringens förslag: Den som tar befattning med en uppgift som har inhämtats genom kamerabevakning får inte obehörigen röja eller utnyttja det som han eller hon har fått veta om någon enskilds personliga förhållanden.

I det allmännas verksamhet ska i stället offentlighets- och sekretesslagen tillämpas.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna tillstyrker förslaget eller har inga synpunkter på det.

Skälen för regeringens förslag: Kameraövervakningslagen innehåller en särskild bestämmelse om tystnadsplikt (37 §). Av bestämmelsen följer att den som tar befattning med en uppgift som har inhämtats genom kameraövervakning inte obehörigen får röja eller utnyttja det som han eller hon på detta sätt har fått veta om någon enskilds personliga förhållanden. Bestämmelsen gäller för privata aktörer. I bestämmelsen upplyses om att i det allmännas verksamhet ska i stället bestämmelserna i offentlighets- och sekretesslagen tillämpas. Vid tolkning av bestämmelsen i kameraövervakningslagen kan ledning sökas i regleringen i offentlighets- och sekretesslagen (2009:400), förkortad OSL.

Enligt offentlighets- och sekretesslagen gäller sekretess för uppgift om en enskilds personliga förhållanden som har inhämtats genom kameraövervakning som avses i kameraövervakningslagen, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men (32 kap. 3 § OSL). Hos en domstol i dess rättskipande eller rättsvårdande verksamhet gäller sekretessen endast om det kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs.

Sekretessen hindrar dock inte att uppgift lämnas till brottsbekämpande myndigheter i vissa fall eller till en kommun eller en myndighet för att förebygga en hotande olycka eller för att begränsa verkningarna av en redan inträffad olycka (32 kap. 3 a § OSL). Sekretess till skydd för en enskild gäller normalt inte heller i förhållande till den enskilde själv (12 kap. 1 § OSL). Det innebär att sekretessen normalt inte hindrar att enskilda kan få tillgång till material från kamerabevakning som avser dem själva i det allmännas verksamhet. Om materialet omfattar även andra

personer, kan den enskilde få tillgång till materialet förutsatt att ett utlämnande inte är till men för någon sådan person eller dennes närstående.

I avsnitt 9 bedöms att rätten till tillgång till personuppgifter enligt dataskyddsförordningen och brottsdatalagen ska gälla som utgångspunkt även vid kamerabevakning. Bestämmelser om sekretess och tystnadsplikt kan emellertid begränsa möjligheten för enskilda att få information om och tillgång till material från kamerabevakning som avser dem själva.

De sekretess- och tystnadspliktsbestämmelser som i dag gäller enligt offentlighets- och sekretesslagen respektive kameraövervakningslagen är avsedda att skydda integriteten hos personer som förekommer i bild- och ljudmaterial. Kameraövervakningslagens bestämmelse om tystnadsplikt innebär ett allmänt förbud mot att obehörigen röja eller utnyttja uppgifter om enskilds personliga förhållanden. Obehörighetsrekvisitet är avsett att tolkas så att ett uppgiftslämnande av en enskild aktör som motsvarar ett uppgiftslämnande som är tillåtet enligt sekretessregleringen inte är att betrakta som obehörigt (se prop. 2012/13:115 s. 104). Det innebär att en behandling som innefattar att bild- och ljudmaterial från kamerabevakning sprids eller lämnas ut till någon annan endast får ske om det står klart att personer som förekommer i materialet eller deras närstående inte lider men.

Dataskyddsförordningen förutsätter att medlemsstaterna kan anta sådana bestämmelser om yrkesmässig eller annan bindande tystnadsplikt (se t.ex. artiklarna 9 och 90). Något hinder mot detta bedöms inte heller finnas enligt det nya dataskyddsdirektivet som tillåter att medlemsstaterna inför starkare skyddsåtgärder.

Kamerabevakningslagen bör därför innehålla en bestämmelse om tystnadsplikt som innebär att den som tar befattning med en uppgift som har inhämtats genom kamerabevakning inte får obehörigen röja eller utnyttja det som han eller hon har fått veta om någon enskilds personliga förhållanden. Den nuvarande bestämmelsen i offentlighets- och sekretesslagen om sekretess för uppgifter om enskildas personliga förhållanden som har inhämtats genom kameraövervakning som avses i kameraövervakningslagen bör ändras så att den i stället gäller för sådan kamerabevakning som avses i kamerabevakningslagen.

11 Tillsyn, sanktioner och rättsmedel

11.1 En tillsynsmyndighet – Datainspektionen

Regeringens förslag: Den myndighet som regeringen bestämmer ska utöva tillsyn över kamerabevakning enligt kamerabevakningslagen.

Regeringens bedömning: Datainspektionen bör vara tillsynsmyndighet enligt kamerabevakningslagen. Detta bör regleras i förordning.

Utredningens förslag och bedömning överensstämmer med regeringens.

Remissinstanserna: En majoritet av remissinstanserna, bl.a. *Datainspektionen*, *Advokatsamfundet*, *Förvaltningsrätten i Umeå*, *Stockholms läns landsting* och *Länsstyrelsen i Dalarna*, tillstyrker förslaget eller har inga synpunkter på det. *Polismyndigheten* avstyrker att Datainspektionen ska vara tillståndsmyndighet eftersom det ökar riskerna för intressekonflikter. Några av länsstyrelserna, bl.a. *Länsstyrelsen i Norrbottens län* och *Länsstyrelsen i Skåne län*, anser att det endast bör vara länsstyrelserna och inte Datainspektionen som ska utöva tillsyn och ansvara för tillståndsprövning enligt den nya lagen. Som skäl för detta anförs bl.a. att länsstyrelserna har en upparbetad kompetens för att fortsätta bedriva tillsynsarbetet samt god lokalkännedom. Enligt *Länsstyrelsen Gävleborg* bör tillsynsansvaret även fortsättningsvis vara delat mellan länsstyrelserna och Datainspektionen.

Skälen för regeringens förslag: I kameraövervakningslagen är tillsynsansvaret delat mellan Datainspektionen och länsstyrelserna. Datainspektionen utövar den operativa tillsynen av kameraövervakning på platser dit allmänheten inte har tillträde och har dessutom det centrala ansvaret för tillsyn enligt lagen. Länsstyrelserna ansvarar för den operativa tillsynen av kameraövervakning på platser dit allmänheten har tillträde. Länsstyrelserna prövar också ansökningar om tillstånd och tar emot sådana anmälningar som innebär att övervakningen får ske utan tillstånd.

Dataskyddsförordningen innehåller en omfattande reglering om tillsyn. Enligt artikel 51 ska varje medlemsstat utse en eller flera självständiga tillsynsmyndigheter som ska ansvara för att övervaka tillämpningen av förordningen. Tillsynsmyndigheten ska enligt artikel 52 vara fullständigt oberoende i utförandet av sina uppgifter och utövandet av sina befogenheter. Enligt artikel 53 ska medlemsstaterna föreskriva att varje ledamot av deras tillsynsmyndigheter ska utnämnas genom ett öppet förfarande. Vidare ska varje ledamot ha de kvalifikationer, den erfarenhet och den kompetens, särskilt på området för skydd av personuppgifter, som krävs för att ledamoten ska kunna utföra sitt uppdrag och utöva sina befogenheter. Tillsynsmyndigheten har de uppgifter som anges i artikel 57, bl.a. att övervaka och verkställa tillämpningen av förordningen, och de befogenheter som anges i artikel 58, bl.a. att besluta om förelägganden och administrativa sanktionsavgifter. Även i dataskyddsdirektivet finns ett flertal bestämmelser om tillsyn (artikel 41–49). I stora delar överensstämmer dessa med eller liknar bestämmelserna i förordningen. Enligt direktivet får det i nationell rätt föreskrivas att en tillsynsmyndighet som har inrättats i enlighet med förordningen ska vara tillsynsmyndighet även enligt direktivet (artikel 41.3).

Tillsynen enligt kamerabevakningslagen måste ordnas på ett sätt som är förenligt med EU-regleringen. Det innebär bl.a. att den myndighet som utövar tillsyn över kamerabevakning måste uppfylla de krav på tillsynsmyndighetens oberoende, organisation och befogenheter som gäller enligt både dataskyddsförordningen och dataskyddsdirektivet. Enligt Utredningen om tillsynen över den personliga integriteten (Ju 2015:02) uppfyller Datainspektionen dessa krav (SOU 2016:65 s. 140–153). Den utredningen föreslår också att Datainspektionen ska utses till svensk tillsynsmyndighet enligt både dataskyddsförordningen och dataskyddsdirektivet, samt att detta ska regleras på förordningsnivå i myndighetens instruktion. Förslagen till dataskyddslag och brottsdatalag

utgår från att tillsynsansvaret enligt dataskyddsförordningen och dataskyddsdirektivet kommer att samlas hos Datainspektionen.

Länsstyrelserna har visserligen en upparbetad kompetens på kameraområdet och en god lokalkännedom som kan vara till nytta både i samband med prövning av tillståndsansökningar och vid tillsynsarbetet. Datainspektionen kommer dock att ha tillsynsansvaret över personuppgiftsbehandling generellt, bl.a. sådan kameraanvändning som inte kommer omfattas av kamerabevakningslagen. Tillsynen över den kamerabevakning som ska omfattas av den nya lagens tillämpningsområde kommer till skillnad från i dag dessutom regelmässigt kräva bedömningar av lagligheten enligt den tillämpliga dataskyddsregleringen, i första hand dataskyddsförordningen och brottsdatalagen. Den ökade rättsliga komplexiteten ställer nya och höga krav på kompetens inom dataskyddsområdet. Den snabba teknikutvecklingen kräver dessutom att en hög teknisk kompetens kan upprätthållas kontinuerligt.

Utredningen bedömer att det är tveksamt om länsstyrelserna i alla delar uppfyller de höga krav som ställs i EU-regleringen på tillsynsmyndighetens roll, organisation och uppgifter. Enligt regeringens bedömning är det uppenbart att länsstyrelserna i dag inte uppfyller dessa krav och att en ordning där länsstyrelserna behåller det särskilda tillsynsansvaret på kameraområdet skulle förutsätta omfattande förändringar av länsstyrelsernas organisation. Det är mot denna bakgrund inte möjligt att, som *Polismyndigheten* förespråkar, låta länsstyrelserna helt eller delvis fortsätta att ansvara för tillståndsprövningen. Inom dataskyddsförordningens tillämpningsområde är det endast den nationella tillsynsmyndigheten som är behörig att pröva frågor om förhandstillstånd och Datainspektionen kommer i egenskap av tillsynsmyndighet enligt brottsdatalagen att vara den myndighet som Polismyndigheten och andra brottsbekämpande myndigheter i övrigt är skyldiga att samråda med.

Även om länsstyrelsernas rättstillämpning synes ha blivit mer enhetlig sedan Datainspektionen fick ett centralt tillsynsansvar enligt kameraövervakningslagen finns dessutom uppenbara fördelar att samla tillsynen hos en myndighet. Utöver vad som framhålls ovan är det viktigt att de förändringar som föreslås genom kamerabevakningslagen får önskade effekter, både när det gäller utökade möjligheter till kamerabevakning och ett förstärkt integritetsskydd. Samtidigt är det angeläget med en enhetlig och korrekt tillämpning av den nya EU-regleringen och den svenska lagstiftningen som rör personuppgiftsbehandling.

Datainspektionen bör därför vara ensam tillsynsmyndighet enligt kamerabevakningslagen. Som utredningen föreslår bör detta regleras i förordning. Kamerabevakningslagen bör därför innehålla en bestämmelse som anger att den myndighet som regeringen bestämmer utövar tillsyn över kamerabevakning enligt kamerabevakningslagen.

11.2 Tillsynsmyndighetens befogenheter och sanktionsavgifter

Regeringens förslag: De bestämmelser om tillsynsmyndighetens befogenheter som gäller enligt EU:s dataskyddsförordning och annan tillämplig personuppgiftsreglering ska gälla även vid tillsynen över att kamerabevakningslagen följs.

Tillsynsmyndigheten ska få ta ut en sanktionsavgift av den som bedriver kamerabevakning och bryter mot lagens bestämmelser om tillståndskrav och upplysningskrav. Detsamma ska gälla för den som inte följer villkor i ett beslut om tillstånd eller ett beslut om undantag från upplysningskravet.

Vid beslut om sanktionsavgift ska bestämmelser i EU:s dataskyddsförordning och dataskyddslagen tillämpas. För kamerabevakning som omfattas av brottsdatalagen ska i stället bestämmelserna i den lagen tillämpas.

Vid överträdelser av kamerabevakningslagens bestämmelser om tillståndskrav ska den lägre avgiftsnivå som föreskrivs i EU:s dataskyddsförordning, eller, i fråga om myndigheter, dataskyddslagen tillämpas. För kamerabevakning som omfattas av brottsdatalagen ska i stället den lägre avgiftsnivå som föreskrivs i den lagen tillämpas.

Vid överträdelser av kamerabevakningslagens bestämmelser om upplysningskrav ska den högre avgiftsnivå som föreskrivs i EU:s dataskyddsförordning, eller, i fråga om myndigheter, dataskyddslagen tillämpas. För kamerabevakning som omfattas av brottsdatalagen ska i stället den högre avgiftsnivå som föreskrivs i den lagen tillämpas.

Regeringens bedömning: Det bör inte införas bestämmelser om straffansvar eller vite i kamerabevakningslagen.

Utredningens förslag och bedömning överensstämmer delvis med regeringens förslag. Utredningen föreslår ingen bestämmelse som anger vilka överträdelser av bestämmelser i kamerabevakningslagen som kan föranleda en sanktionsavgift och inte heller bestämmelser om vilken avgiftsnivå som aktualiseras vid respektive överträdelse. Utredningen föreslår i stället en bestämmelse om att den högre avgiftsnivån ska gälla för myndigheter vid överträdelser av regleringen i kamerabevakningslagen.

Remissinstanserna: En majoritet av remissinstanserna tillstyrker förslaget eller har inga synpunkter på det. *Datainspektionen* ifrågasätter i vilken mån sanktionsavgifter kommer kunna dömas ut för överträdelser av bestämmelserna i kamerabevakningslagen med hänsyn till regelsystemets komplexitet och vissa oklarheter som rör det tillståndspliktiga området. Datainspektionen anser vidare att den av utredningen föreslagna bestämmelsen är otydlig och svår att förstå samt efterlyser ett förtydligande av vilka bestämmelser i dataskyddsförordningen som ska tillämpas när de olika reglerna i kamerabevakningslagen överträds och vilka avgiftsnivåer som blir aktuella för andra än myndigheter. Några remissinstanser, däribland *Polismyndigheten* och *Försvarsmakten*, motsätter sig att myndigheter ska kunna bli föremål för sanktionsavgifter. *Karlskrona kommun* anser i och för sig att det är rimligt att myndigheter kan drabbas av sanktionsavgifter vid överträdelser men påpekar att den

högre avgiftsnivå som utredningen föreslår kraftigt avviker från liknande högsta sanktionsbelopp i svensk rätt.

Skälen för regeringens förslag

Tillsynsmyndighetens befogenheter

Enligt kameraövervakningslagen har länsstyrelserna och Datainspektionen vissa befogenheter i sin tillsynsverksamhet, bl.a. att meddela förelägganden och förena dessa med vite (41 och 42 §§). Tillsynsmyndigheterna har också rätt att få tillträde till övervakningsanläggningar och Polismyndigheten är skyldig att på begäran lämna den handräckning som dessa myndigheter behöver för att få tillträde (43 §).

Dataskyddsförordningen innehåller en omfattande och direkt tillämplig reglering av vilka befogenheter som tillsynsmyndigheten ska ha (artikel 58). Tillsynsmyndigheten har dels vissa utredningsbefogenheter, bl.a. en rätt att beordra den personuppgiftsansvarige eller personuppgiftsbiträdet att lämna all information som myndigheten behöver för att kunna fullgöra sina uppgifter. Som ett led i sina utredningar har tillsynsmyndigheten också rätt att få tillträde till lokaler som tillhör en personuppgiftsansvarig eller ett personuppgiftsbiträde, inklusive tillgång till utrustning och andra medel för behandling av personuppgifter i överenstämmelse med nationell processrätt. Tillsynsmyndigheten har vidare vissa korrigerande befogenheter, bl.a. kan myndigheten utfärda varningar om att planerade behandlingar sannolikt kommer att bryta mot förordningen och meddela förelägganden om att en behandling ska ske i enlighet med bestämmelserna i förordningen. Tillsynsmyndigheten kan också tillfälligt eller definitivt begränsa, inklusive förbjuda, en behandling av personuppgifter. Även det nya dataskyddsdirektivet innehåller bestämmelser om tillsyn som till stora delar har samma eller liknande innehåll som bestämmelserna i förordningen och som kommer att genomföras i svensk rätt genom brottsdatalagen.

Utredningen om tillsynen över den personliga integriteten bedömer att det saknas behov av att föreskriva ytterligare befogenheter för tillsynsmyndigheten utöver vad som följer av den nya EU-regleringen (SOU 2016:65 s. 154–157). Utredningens förslag bereds i Regeringskansliet.

Det är angeläget att tillsynsmyndigheten har samma tillsynsbefogenheter enligt kamerabevakningslagen som vid personuppgiftsbehandling generellt. Dataskyddslagen föreslås visserligen innehålla en bestämmelse som innebär att de befogenheter som tillsynsmyndigheten har enligt dataskyddsförordningen också gäller vid tillsyn över efterlevnaden av bestämmelserna i författningar som kompletterar dataskyddsförordningen (6 kap. 1 §). Någon motsvarande bestämmelse finns dock inte i förslaget till brottsdatalag och det är fortfarande ovisst hur framtida personuppgiftsregleringar på området utanför EU-rättens tillämpningsområde kommer att se ut.

Det bör därför tas in en bestämmelse i kamerabevakningslagen om att de befogenheter som tillsynsmyndigheten, dvs. Datainspektionen, har enligt dataskyddsförordningen och annan tillämplig personuppgiftsreglering, t.ex. brottsdatalagen, gäller även vid tillsynen

över att kamerabevakningslagen följs. Detta innebär bl.a. att tillsynsmyndigheten kan använda de nämnda befogenheterna i samband med handläggning av ärenden enligt lagen eller när den som bedriver kamerabevakningen underlåter att bistå myndigheten i ett sådant ärende.

Regleringen i dataskyddsförordningen och brottsdatalagen ger tillsynsmyndigheten rätt att få tillträde till den personuppgiftsansvariges eller personuppgiftsbiträdets lokaler. I propositionen Ny dataskyddslag bedömer regeringen att det inte behövs några kompletterande bestämmelser i dataskyddslagen som ger tillsynsmyndigheten möjlighet att tillgripa tvångsåtgärder för att genomföra en sådan platsundersökning. I propositionen konstateras att en undersökning av lokalerna i de allra flesta fall bör kunna ske med innehavarens medgivande samt att risken för att tillsynsmyndigheten annars beslutar om tillfälligt förbud mot behandlingen torde medföra att innehavaren ger tillsynsmyndigheten det tillträde den har rätt till. Det framhålls vidare att en underlåtelse att rätta sig efter ett föreläggande eller att ge tillsynsmyndigheten tillgång till uppgifter kan medföra att sanktionsavgifter tas ut (se prop. 2017/18:105 s. 157–158). Det saknas anledning att göra en annan bedömning i detta lagstiftningsärende. Några särskilda bestämmelser om handräckning bör därför inte införas i kamerabevakningslagen.

Regleringen om sanktionsavgifter

Enligt artikel 58.2 i dataskyddsförordningen ska tillsynsmyndigheten vid överträdelser av förordningens bestämmelser ha befogenhet att utöver eller i stället för andra korrigerande befogenheter påföra administrativa sanktionsavgifter. Sanktionsavgifter kan också påföras vid underlåtenhet att rätta sig efter vissa av tillsynsmyndighetens förelägganden eller beslut. I de sistnämnda fallen fyller sanktionsavgiften en vitesliknande funktion.

Enligt artikel 83.1 i dataskyddsförordningen ska varje tillsynsmyndighet säkerställa att påförande av administrativa sanktionsavgifter i varje enskilt fall är effektivt, proportionellt och avskräckande. Vid beslut om huruvida en administrativ sanktionsavgift ska påföras och hur stort belopp avgiften ska uppgå till ska, enligt artikel 83.2 i förordningen, bl.a. beaktas överträdelsens karaktär, svårighetsgrad och varaktighet, om överträdelsen skett med uppsåt eller av oaktsamhet samt graden av samarbete med tillsynsmyndigheten för att komma till rätta med överträdelsen och minska dess potentiella negativa effekter.

För vissa mindre allvarliga överträdelser, såsom överträdelse av kravet på konsekvensbedömning eller underlåtelse att samråda med tillsynsmyndigheten, är maxbeloppet för sanktionsavgiften enligt artikel 83.4 i dataskyddsförordningen 10 miljoner euro eller två procent av den globala årsomsättningen när det gäller företag, beroende på vilket belopp som är högst. För allvarligare överträdelser, t.ex. överträdelse av de grundläggande principerna för behandling, rätten till information eller underlåtenhet att rätta sig efter tillsynsmyndighetens förelägganden, är, enligt artikel 83.5, maxbeloppet 20 miljoner euro eller fyra procent av den globala årsomsättningen. Om en personuppgiftsansvarig eller ett personuppgiftsbiträde överträder flera av bestämmelserna i förordningen får, enligt artikel 83.3, sanktionsavgiftens totala belopp inte överstiga det belopp som fastställs för den allvarligaste överträdelsen.

Enligt förslaget till dataskyddslag ska sanktionsavgifter även få tas ut av en myndighet vid överträdelser som avses i dataskyddsförordningen. Avgiftens storlek för myndigheter ska uppgå till högst 10 miljoner kronor för de mindre allvarliga överträdelserna och högst 20 miljoner kronor för de allvarligare överträdelserna (6 kap. 2 §). Förslaget till dataskyddslag innehåller också vissa bestämmelser om förfarandet vid beslut om sanktionsavgifter och om betalning av avgifterna (6 kap. 4–7 §§).

Ett motsvarande system med sanktionsavgifter föreslås gälla inom det nya dataskyddsdirektivets tillämpningsområde genom regleringen i brottsdatalagen. Avgifterna ska enligt förslaget bestämmas till högst 5 miljoner kronor vid vissa mindre allvarliga överträdelser och högst 10 miljoner kronor för de allvarligare överträdelserna.

De grundläggande förutsättningarna för kamerabevakning kommer framöver främst att styras av regleringen i dataskyddsförordningen och, för sådan kamerabevakning som omfattas av det nya dataskyddsdirektivet, brottsdatalagen. Det innebär att förordningens och brottsdatalagens regler om sanktionsavgifter kommer att bli tillämpliga vid sådan kamerabevakning som t.ex. strider mot grundläggande principer för personuppgiftsbehandling eller saknar rättslig grund.

Vilka överträdelser bör kunna leda till sanktionsavgifter?

Den materiella regleringen i kamerabevakningslagen kommer att vara mer begränsad än den nuvarande regleringen i kameraövervakningslagen. Den centrala materiella regleringen i lagen är dels bestämmelserna om krav på tillstånd och dels bestämmelserna om krav på upplysning. Som utredningen föreslår bör sanktionsavgifterna gälla vid överträdelser av dessa bestämmelser i lagen och vid överträdelser av villkor i sådana beslut som meddelats med stöd av lagen.

Liksom i dataskyddslagen bör hänvisningar till dataskyddsförordningens bestämmelser om sanktionsavgifter vara statiska, dvs. avse förordningen i den ursprungliga lydelsen. Detta med hänsyn till behovet av förutsebarhet i fråga om vilka sanktioner som kan bli följden av överträdelser.

Som *Datainspektionen* anför kan det uppkomma fall där det är oklart hur kamerabevakningslagen ska tolkas. I sådana fall bör den som har gjort en felaktig tolkning av regleringen först ges möjlighet att komma till rätta med överträdelsen genom exempelvis ett föreläggande eller en varning från tillsynsmyndigheten. Först om en sådan varning eller ett sådant föreläggande inte följs bör sanktionsavgifter komma i fråga. En sådan ordning överensstämmer väl med regleringen i både dataskyddsförordningen och det nya dataskyddsdirektivet som innebär att vederbörlig hänsyn i varje enskilt fall måste tas till bl.a. överträdelsens karaktär, om den skett med uppsåt eller genom oaktsamhet samt graden av samarbete med tillsynsmyndigheten.

Sanktionsavgifter ska kunna tas ut av myndigheter

Vissa remissinstanser invänder mot att myndigheter ska kunna drabbas av sanktionsavgifter. Det kan dock konstateras att regeringens förslag till dataskyddslag och brottsdatalag innehåller bestämmelser om sanktionsavgifter för myndigheter. Vidare är den nuvarande regleringen

utformad så att sanktionssystemet är enhetligt för myndigheter och enskilda. Kameraövervakningslagens bestämmelser om straff och viten omfattar således både myndigheter och enskilda. Enligt regeringens bedömning bör även den nya lagens sanktioner vara likartade för myndigheter och privata organ. Regeringen instämmer därför i utredningens bedömning att sanktionsavgifter ska kunna påföras även myndigheter. Det bör understrykas att detta inte innebär ett ställningstagande i frågan om hur regleringen om sanktioner bör se ut i kommande personuppgiftsreglering för myndigheter inom området för nationell säkerhet, exempelvis Säkerhetspolisen och Försvarsmakten.

Bestämmelser om förfarandet

Det bör framgå av kamerabevakningslagen vilka bestämmelser som ska gälla vid förfarandet rörande sanktionsavgifter. Detta sker lämpligast genom hänvisning till relevanta bestämmelser i dataskyddslagen och brottsdatalagen Det bör således framgå att dataskyddslagens bestämmelser om förfarandet (6 kap. 4–7 §§) ska tillämpas vid beslut om sanktionsavgifter. För kamerabevakning som omfattas av brottsdatalagen ska i stället motsvarande bestämmelser om förfarandet i brottsdatalagen (6 kap. 6–9 §§) tillämpas. Detta innebär att dataskyddslagens reglering om förfarandet, i enlighet med utredningens förslag, också gäller för sådan kamerabevakning som inte omfattas av EU-rättens tillämpningsområde.

Det bör vidare framgå av kamerabevakningslagen vilka bestämmelser som ska gälla vid bedömningen av om en sanktionsavgift ska tas ut och de omständigheter som ska beaktas när storleken på avgiften ska bestämmas. Detta sker lämpligast genom hänvisning till relevanta bestämmelser i dataskyddsförordningen och brottsdatalagen. Det bör således framgå av kamerabevakningslagen att artikel 83.1, 83.2 och 83.3 i EU:s dataskyddsförordning ska tillämpas vid beslut om sanktionsavgift. För sådan kamerabevakning som omfattas av brottsdatalagen ska motsvarande bestämmelser i den lagen tillämpas i stället (6 kap. 3 § tredje stycket samt 4 och 5 §§). Dataskyddsförordningens och dataskyddslagens reglering bör, i enlighet med utredningens förslag, även i detta avseende gälla för sådan kamerabevakning som inte omfattas av EU-rättens tillämpningsområde.

Avgiftsnivåerna

Regeringen anser, till skillnad från utredningen, att nivån på sanktionsavgifterna av enhetlighetsskäl bör vara densamma vid överträdelser av kamerabevakningslagen som vid överträdelser av motsvarande bestämmelser i den generella personuppgiftsregleringen. Regeringen delar vidare *Datainspektionens* uppfattning att det finns ett behov av att förtydliga utredningens förslag och att det i kamerabevakningslagen uttryckligen bör anges vilka överträdelser som kan aktualisera en sanktionsavgift och vilken avgiftsnivå som i så fall ska tillämpas. Detta bör ske genom att hänvisning sker till de avgiftsnivåer som gäller enligt dataskyddsförordningen, dataskyddslagen och brottsdatalagen. Dataskyddsförordningens och dataskyddslagens reglering om avgiftsnivåer bör därvid gälla även för sådan kamerabevakning som inte omfattas av EU-rättens tillämpningsområde.

Tillståndskravet för kamerabevakning utgör en precisering av kravet på konsekvensbedömning och samråd med tillsynsmyndigheten i artiklarna 35.1 och 36.1 i dataskyddsförordningen. Överträdelser av dessa bestämmelser är enligt förordningen sanktionerade med den lägre avgiftsnivån i artikel 83.4. Enligt förslaget till brottsdatalag gäller också motsvarande lägre avgiftsnivå för överträdelser av lagens bestämmelser om konsekvensbedömning och samrådsskyldighet. Kamerabevakningslagen bör därför innehålla en bestämmelse som anger att den lägre avgiftsnivå som föreskrivs i dataskyddsförordningen, eller, i fråga om myndigheter, dataskyddslagen, ska tillämpas vid överträdelser av lagens bestämmelser som rör tillståndskravet. För kamerabevakning som omfattas av brottsdatalagen ska i stället den lägre avgiftsnivå som föreskrivs i den lagen tillämpas.

Att underlåta att upplysa om kamerabevakning innebär normalt också ett åsidosättande av enskildas rätt till information om den personuppgiftsbehandling som bevakningen innebär. Överträdelser av kamerabevakningslagens upplysningskrav bör därmed jämställas med sådana överträdelser av bestämmelserna om de registrerades rättigheter som omfattas av den högre avgiftsnivån i artikel 83.5 dataskyddsförordningen.

Enligt förslaget till brottsdatalag ska överträdelser av de bestämmelser som reglerar enskildas rätt till information i och för sig inte vara föremål för sanktionsavgifter. Anledningen till detta är att den allmänna information som ska lämnas enligt brottsdatalagen inte bedöms vara av sådan karaktär att det finns någon större risk att en registrerad lider rättsförlust om informationen inte lämnas, samt att skyldigheten att lämna personrelaterad information i specifika fall förutsätter en bedömning av när information ska lämnas (SOU 2017:29 s. 509–510). Förhållandena vid kamerabevakning är emellertid speciella. Huvudregeln att upplysning ska lämnas vid kamerabevakning är av grundläggande betydelse för integritetsskyddet och utgör även en viktig avgränsning i förhållande till regleringen om hemlig kameraövervakning. I kameraövervakningslagen är upplysningskravet straffsanktionerat och det är enligt regeringen inte lämpligt att låta överträdelser av kravet på upplysning i den nya lagen helt eller delvis vara fritt från sanktioner. Sanktionsavgifter bör därför även kunna tas ut vid överträdelser av upplysningskravet vid sådan kamerabevakning som omfattas av det nya dataskyddsdirektivet.

Mot denna bakgrund bör det framgå av en bestämmelse i kamerabevakningslagen att den högre avgiftsnivån i dataskyddsförordningen, eller, i fråga om myndigheter, i dataskyddslagen ska tillämpas vid överträdelser av bestämmelserna i lagen som rör upplysningskravet. För kamerabevakning som omfattas av brottsdatalagen ska i stället den högre avgiftsnivå som föreskrivs i den lagen tillämpas.

Det bör inte införas några bestämmelser om straff eller vite

Varken dataskyddslagen eller brottsdatalagen innehåller några straffbestämmelser eller bestämmelser om vite. Som konstateras ovan kan sanktionsavgifterna användas framåtsyftande och utdömas t.ex. om ett föreläggande inte följs. I dessa fall har sanktionsavgiften en vitesliknande funktion. Det kan vidare konstateras att den nuvarande straffbestämmelsen

i kameraövervakningslagen tillämpas mycket sällan och det får förutsättas vara mer effektivt och verkningsfullt att i stället ge tillsynsmyndigheten möjlighet att direkt sanktionera överträdelser. Att behålla ett särskilt straffansvar för regleringen i kamerabevakningslagen skulle dessutom riskera att aktualisera det s.k. dubbelbestraffningsförbudet som finns både i Europakonventionen och i Europeiska unionens stadga om de grundläggande rättigheterna. Regeringen instämmer mot denna bakgrund i utredningens bedömning att kamerabevakningslagen inte bör innehålla några bestämmelser om straff och viten.

11.3 Skadestånd

Regeringens förslag: Vid överträdelse av bestämmelser i kamerabevakningslagen eller av beslut som meddelats med stöd av lagen ska bestämmelser om rätt till ersättning i EU:s dataskyddsförordning tillämpas. För kamerabevakning som omfattas av brottsdatalagen ska i stället bestämmelserna om skadestånd i den lagen tillämpas.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Sveriges advokatsamfund* ifrågasätter om den svenska rätten att föra talan om skadestånd vid allmän domstol utgör ett sådant effektivt rättsmedel för enskilda som EU-regleringen kräver eftersom skadeståndsnivåerna i svensk rätt är så låga att enskilda exempelvis inte ges möjlighet att ta i anspråk rättsskyddet i sin hemförsäkring vid en sådan process. Även *Tjänstemännens centralorganisation (TCO)* framhåller att de ideella skadeståndsnivåerna i svensk rätt är låga.

Skälen för regeringens förslag: Enligt 44 § kameraövervakningslagen ska den som bedriver kameraövervakning ersätta den övervakade för skada och kränkning av den personliga integriteten som kameraövervakning i strid med lagen har orsakat. Ersättningsskyldigheten kan i den utsträckning det är skäligt jämkas, om den som har bedrivit övervakningen visar att felet inte berodde på honom eller henne.

Enligt artikel 82 i dataskyddsförordningen ska varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av förordningen ha rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den uppkomna skadan. Möjligheten att få ersättning för immateriell skada får anses motsvara möjligheten att få kränkningsersättning enligt kamerabevakningslagen. Dataskyddsförordningens bestämmelse om ersättning tar över de allmänna skadeståndsreglerna i skadeståndslagen (1972:207) (1 kap. 1 § skadeståndslagen).

Enligt ordalydelsen i artikel 82 i dataskyddsförordningen gäller rätten till ersättning vid skada som uppstått till följd av behandling som strider mot dataskyddsförordningen. Enligt skäl 146 till förordningen gäller dock rätten till ersättning även vid behandling som strider mot nationella bestämmelser som specificerar förordningen. I förslaget till dataskyddslag har regeringen ansett att detta bör förtydligas genom en bestämmelse som anger att rätten till ersättning gäller vid överträdelser av bestämmelser i

dataskyddslagen och i andra författningar som kompletterar dataskyddsförordningen (7 kap. 1 §). Kamerabevakningslagen kommer att innehålla bestämmelser som kompletterar dataskyddsförordningen. När det gäller sådana bestämmelser behövs ingen särskild reglering om rätten till ersättning.

Förslaget till brottsdatalag innehåller också bestämmelser som anger att den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som har orsakats av behandling av personuppgifter i strid med lagen, eller föreskrifter som har meddelats i anslutning till den (7 kap. 1 §) Bestämmelsen har sin grund i artikel 56 i det nya dataskyddsdirektivet. Eftersom bestämmelsen i brottsdatalagen tar sikte på sådan skada och kränkning som personuppgiftsbehandling i strid med bestämmelserna i just den lagen innebär kan det hävdas att den inte utan särskild reglering även gäller vid överträdelser av bestämmelser i kamerabevakningslagen.

Kamerabevakningslagen bör därför innehålla en bestämmelse som anger att brottsdatalagens reglering om rätt till ersättning ska tillämpas vid överträdelser i samband med kamerabevakning som omfattas av den lagen. Av tydlighetsskäl bör bestämmelsen ges en mer generell utformning och även upplysa om vad som gäller vid överträdelser i samband med kamerabevakning inom dataskyddsförordningens tillämpningsområde. Dataskyddsförordningens reglering om rätt till ersättning bör vidare, i enlighet med utredningens förslag, även tillämpas vid sådan kamerabevakning som inte omfattas av EU-rättens tillämpningsområde.

Mot denna bakgrund bör kamerabevakningslagen innehålla en bestämmelse som anger att dataskyddsförordningens bestämmelser om rätt till ersättning ska tillämpas vid överträdelser av bestämmelser i lagen och vid beslut som har meddelats med stöd av lagen. För kamerabevakning som omfattas av brottsdatalagen ska i stället den lagens bestämmelser om skadestånd tillämpas.

I enlighet med den bedömning som har gjorts i förslagen till dataskyddslag och brottsdatalagen anser regeringen, till skillnad från *Sveriges advokatsamfund*, att rätten till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde tillgodoses i svensk rätt genom möjligheten att vid allmän domstol föra talan om ersättning.

11.4 Överklagande

Regeringens förslag: Tillsynsmyndighetens beslut enligt kamerabevakningslagen ska få överklagas till allmän förvaltningsdomstol. När ett beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Beslut om tillstånd till kamerabevakning och om undantag från kravet på upplysning ska få överklagas även av den kommun där bevakningen ska ske och, om kamerabevakningen ska avse en arbetsplats, av en organisation som företräder arbetstagarna på arbetsplatsen.

Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår ingen bestämmelse om att tillsynsmyndigheten är motpart i domstolen när myndighetens beslut överklagas.

Remissinstanserna: *Datainspektionen* anser att det bör införas en möjlighet för Justitiekanslern eller någon annan myndighet att överklaga beslut om tillstånd enligt kamerabevakningslagen för att ta tillvara allmänna intressen. *Kammarrätten i Stockholm* anser att det finns anledning att överväga om det bör införas en särskild bestämmelse i lagen om att tillsynsmyndigheten är motpart om dess beslut överklagas. Kammarrätten anser vidare att det mot bakgrund av vissa uttalanden i förarbetena till den nya förvaltningslagen (2017:900) kan finnas anledning att beröra frågan om en myndighets klagorätt. *Kammarrätten i Sundsvall* ifrågasätter lämpligheten av att ärenden som överklagas ska fokuseras till en förvaltningsrätt respektive en kammarrätt i landet. *Förvaltningsrätten i Umeå* anser att det bör övervägas om de aktuella målen i stället bör prövas av en förvaltningsrätt utanför Stockholmsområdet.

Skälen för regeringens förslag: Som framgår av avsnitt 11.1 kommer tillsynsmyndighetens beslut vid kamerabevakning i stor utsträckning fattas genom en direkt tillämpning av bestämmelser i annan dataskyddsreglering. Vid överklagande av sådana beslut kommer också bestämmelserna om överklagande i den aktuella dataskyddsregleringen att bli tillämpliga. Om tillsynsmyndigheten exempelvis beslutar om en administrativ sanktionsavgift på grund av att material från kamerabevakningen inte behandlas i enlighet med regleringen i dataskyddsförordningen eller brottsdatalagen, gäller därmed bestämmelser om överklagande i förordningen och dataskyddslagen, respektive brottsdatalagen. Detta framgår av den bestämmelse om kamerabevakningslagens förhållande till annan dataskyddsreglering som föreslås i avsnitt 5.3.2.

När det gäller sådana frågor som regleras direkt i kamerabevakningslagen, t.ex. frågor om tillstånd till kamerabevakning och undantag från upplysningskravet, bör det även fortsättningsvis vara möjligt att överklaga sådana beslut till allmän förvaltningsdomstol. Ett överklagande till kammarrätten bör kräva prövningstillstånd. Liksom enligt den nuvarande kameraövervakningslagen bör vissa beslut även få överklagas av den kommun där bevakningen ska ske och, om kamerabevakningen ska avse en arbetsplats, av en organisation som företräder arbetstagarna på arbetsplatsen.

Med anledning av synpunkterna från *Kammarrätten i Stockholm* kan konstateras att, enligt såväl personuppgiftslagen som kameraövervakningslagen, anses personuppgiftsansvariga myndigheter ha rätt att överklaga tillsynsmyndigheternas beslut till allmän förvaltningsdomstol. Detta är dessutom en nödvändig följd av kravet på effektiva rättsmedel i såväl dataskyddsförordningen som det nya dataskyddsdirektivet. Någon förändring av denna ordning är inte avsedd.

Regeringen instämmer i utredningens bedömning att den nya förvaltningslagen och förvaltningsprocesslagen (1971:291) innehåller ändamålsenliga bestämmelser om i vilka fall tillsynsmyndighetens beslut får verkställas omedelbart respektive inhiberas av domstol. Några särskilda bestämmelser om detta bör därför inte tas in i kamerabevakningslagen. Det bör dock framhållas att det i regel bör finnas

anledning för tillsynsmyndigheten att bestämma att ett positivt beslut om tillstånd till kamerabevakning ska gälla omedelbart eftersom ett sådant beslut i normalfallet inte kommer att överklagas.

Av 14 § andra stycket lagen (1971:289) om allmänna förvaltningsdomstolar följer att ett beslut ska överklagas till den förvaltningsrätt inom vars domkrets ärendet först prövats, om det inte för ett visst slag av mål föreskrivs annat i lag eller förordning. Eftersom beslut i ärenden enligt kamerabevakningslagen endast kommer att meddelas av Datainspektionen kommer handläggningen av överklagade beslut att koncentreras till en förvaltningsrätt och en kammarrätt. Som bl.a. *Kammarrätten i Sundsvall* framhåller finns det skäl att överväga lämpligheten av en sådan ordning. Regeringen kan dock konstatera att överklaganden av Datainspektionens beslut i andra frågor enligt dataskyddsförordningen, dataskyddslagen eller brottsdatalagen kommer att koncentreras till samma domstolar. Att ha en särskild överklagandeordning för regleringen i kamerabevakningslagen skulle riskera att skapa svåra gränsdragningsfrågor när överklagade beslut rör tillämpning av både kamerabevakningslagen och annan dataskyddsreglering. Skälen för att samla tillsynen hos Datainspektionen talar också för att prövningen hos domstol bör koncentreras (se avsnitt 11.1). Exempelvis förbättras förutsättningarna att snabbare få till stånd en enhetlig rättstillämpning inom ett förhållandevis komplext rättsområde.

Regeringen instämmer därför i utredningens bedömning att det inte finns anledning att införa en särskild reglering som innebär behörighet för flera domstolar i frågor som regleras i kamerabevakningslagen. Överklaganden av tillsynsmyndighetens beslut enligt kamerabevakningslagen kommer därmed, liksom beslut enligt övrig dataskyddsreglering, att kunna överklagas till Förvaltningsrätten i Stockholm och därefter till Kammarrätten i Stockholm.

Regeringen ser, till skillnad från *Datainspektionen*, inget behov av att ge Justitiekanslern eller någon annan myndighet rätt att överklaga Datainspektionens beslut för att ta tillvara allmänna intressen. En sådan rätt för Justitiekanslern har funnits i äldre lagstiftning på området men ansågs ha spelat ut sin roll i samband med införandet av Datainspektionens centrala tillsynsansvar som innefattar en möjlighet att överklaga principiellt viktiga beslut. Datainspektionens centrala tillsynsansvar infördes bl.a. för att komma till rätta med en bristande enhetlighet i länsstyrelsernas praxis (se prop. 2012/13:115 s. 129–134). Eftersom regeringens förslag innebär att prövningen av ärenden enligt kamerabevakningslagen ska samlas hos en myndighet kommer det inte finnas ett behov av att en annan myndighet ges en klagorätt i syfte att åstadkomma en enhetlig praxis. Vidare kommer Datainspektionen, som framgår av avsnitt 11.1, ha som uppgift att se till att dataskyddsregleringen efterlevs i medlemsstaterna. Det är därför inte lämpligt att någon annan myndighet ges möjlighet att överklaga Datainspektionens beslut i syfte att bevaka det allmänna intresset av att skydda den personliga integriteten. När det gäller det allmänna intresset av att kamerabevakning kan ske för berättigade ändamål kan detta intresse tillgodoses i tillräcklig utsträckning genom att den som bedriver kamerabevakningen kan överklaga beslut som begränsar möjligheten att kamerabevaka. Datainspektionen kommer dessutom att ha möjlighet att överklaga domstolarnas avgöranden. Av

tydlighetsskäl bör det som Kammarrätten i Stockholm påpekar dock framgå av kamerabevakningslagen att tillsynsmyndigheten har ställning som motpart när myndighetens beslut överklagas till domstol. En motsvarande bestämmelse finns också i förslaget till dataskyddslag (7 kap. 3 §).

11.5 Föreskriftsrätt för tillsynsmyndigheten

Regeringens bedömning: Någon rätt för tillsynsmyndigheten att meddela föreskrifter som rör tillämpningen av kamerabevakningslagen behövs inte. Kamerabevakningslagen bör inte heller innehålla någon föreskriftsrätt för regeringen eller tillsynsmyndigheten angående avgifter för ansökningar enligt lagen.

Utredningens bedömning överensstämmer delvis med regeringens. Utredningen föreslår att det i kamerabevakningslagen ska införas en föreskriftsrätt för regeringen eller den myndighet som regeringen bestämmer som avser avgifter för ansökningar enligt lagen.

Remissinstanserna: Enligt *Datainspektionen* är det inte förenligt med EU-regleringen att ta ut ansökningsavgifter av det aktuella slaget och det vore dessutom olämpligt eftersom avgifterna främst skulle drabba andra myndigheter och innebära en omfattande administration för inspektionen. Datainspektionen avstyrker därför utredningens förslag i denna del.

Skälen för regeringens bedömning: I lagstiftningsärendet om kameraövervakningslagen väckte flera remissinstanser frågan om den centrala tillsynsmyndigheten borde ges en rätt att meddela föreskrifter för tillämpningen av lagen (se prop. 2012:13/115 s. 132). Någon föreskriftsrätt infördes dock inte.

I förslagen till dataskyddslag och brottsdatalag ges en relativt omfattande föreskriftsrätt för Datainspektionen på dataskyddsområdet. Denna föreskriftsrätt kommer gälla även för kamerabevakning i de frågor som inte regleras direkt i kamerabevakningslagen. Vidare bör det förhållandet att tillsynen samlas hos en myndighet och att beslut kan överprövas av ett fåtal domstolar leda till en mer enhetlig tillämpning av reglerna än i dag. Dessutom ingår det i tillsynsmyndighetens uppgifter enligt dataskyddförordningen att öka medvetenheten om regelverket och bl.a. främja framtagandet av uppförandekoder inom olika sektorer som ska bidra till att reglerna tillämpas korrekt. Mot den bakgrunden instämmer regeringen i utredningens bedömning att det inte behövs någon föreskriftsrätt för tillsynsmyndigheten när det gäller de materiella bestämmelserna i kamerabevakningslagen.

Regeringen delar *Datainspektionens* uppfattning att det kan ifrågasättas om det finns utrymme enligt EU-regleringen att ta ut ansökningsavgifter på det sätt som utredningen föreslår. Eftersom antalet ärenden om tillstånd kan förväntas bli betydligt färre än tidigare skulle det vidare handla om ett förhållandevis litet finansiellt tillskott för staten. En avgiftsfinansiering skulle dessutom innebära en tillkommande administrativ börda för tillsynsmyndigheten. Någon föreskriftsrätt om ansökningsavgifter bör mot denna bakgrund inte införas.

12 Ikraftträdande- och övergångsbestämmelser

Regeringens förslag: Kamerabevakningslagen och ändringen i offentlighets- och sekretesslagen ska träda i kraft den 1 augusti 2018 samtidigt som kameraövervakningslagen ska upphöra att gälla.

Tillstånd till kameraövervakning som har beslutats enligt kameraövervakningslagen och som avser kamerabevakning som omfattas av kravet på tillstånd i den nya lagen ska fortfarande gälla. Övriga tillstånd som har beslutats enligt kameraövervakningslagen ska inte längre gälla.

Anmälningar som har gjorts enligt kameraövervakningslagen ska inte längre gälla.

Beslut om undantag från upplysningskravet som har fattats enligt kameraövervakningslagen ska gälla som ett beslut om undantag från upplysningskravet och rätten till information enligt den nya lagen.

Ärenden som har inletts hos länsstyrelserna enligt kameraövervakningslagen men ännu inte har avgjorts ska överlämnas till den myndighet som ska utöva tillsyn över kamerabevakning enligt den nya lagen.

Om ett beslut som har fattats enligt den upphävda lagen har överklagats av någon annan än tillsynsmyndigheten enligt den nya lagen, ska tillsynsmyndigheten vara motpart i målet.

Äldre föreskrifter om straff ska fortfarande gälla för överträdelser som har skett före ikraftträdandet.

I fråga om ändringen i offentlighets- och sekretesslagen ska äldre föreskrifter fortfarande gälla för uppgifter som har inhämtats före ikraftträdandet.

Utredningens förslag överensstämmer i huvudsak med regeringens. Enligt utredningens förslag ska mål som har överklagats enligt kameraövervakningslagen till en annan förvaltningsrätt än Förvaltningsrätten i Stockholm eller till en annan kammarrätt än Kammarrätten i Stockholm men ännu inte har avgjorts, överlämnas till Förvaltningsrätten i Stockholm respektive Kammarrätten i Stockholm. Utredningen föreslår också en särskild övergångsbestämmelse för skadestånd för sådan skada som orsakats före ikraftträdandet.

Remissinstanserna: *Datainspektionen* ifrågasätter om det är praktiskt möjligt att låta äldre tillstånd om kameraövervakning fortsätta gälla i de fall de avser sådan kamerabevakning som omfattas av tillståndskrav enligt den nya lagen. Enligt Datainspektionen kommer tillståndsprövningen enligt kamerabevakningslagen att omfatta en bedömning av huruvida bevakningen är laglig enligt dataskyddsförordningen eller brottsdatalagen, vilket är en mer omfattande prövning än den som länsstyrelsen gör enligt kameraövervakningslagen. Det kan enligt Datainspektionen därför inte presumeras att de tillstånd som har beviljats enligt kameraövervakningslagen uppfyller dataskyddsförordningens respektive brottsdatalagens krav. *Kammarrätten i Stockholm* anser att det bör övervägas om bestämmelsen bör ändras för att säkerställa att Datainspektionen blir motpart i samtliga mål där det överklagade beslutet

har fattats av en länsstyrelse och inte bara i de fall där en enskild överklagat beslutet. Kammarrätten kan också se ett behov av att förtydliga vad som gäller om tillsynsmyndighetens beslut om ett föreläggande vid äventyr av vite har överklagats och det pågår en process i domstol när kameraövervakningslagen upphör att gälla.

Skälen för regeringens förslag

Ikraftträdande

Av artikel 99 i dataskyddsförordningens följer att förordningen ska tillämpas från och med den 25 maj 2018. Dataskyddslagen föreslås träda i kraft den dagen samtidigt som personuppgiftslagen ska upphöra att gälla. Enligt artikel 63 i det nya dataskyddsdirektivet ska medlemsstaterna senast den 6 maj 2018 anta och offentliggöra de lagar och andra författningar som är nödvändiga för att genomföra direktivet. Bestämmelserna ska tillämpas av medlemsstaterna från och med samma dag. Brottsdatalagen föreslås träda i kraft den 1 augusti 2018.

Kamerabevakningslagen bör träda i kraft så snart som möjligt. Lagen innehåller emellertid bestämmelser som både kompletterar dataskyddsförordningen och genomför det nya dataskyddsdirektivet. Vissa av lagens bestämmelser hänvisar dessutom direkt till dataskyddsförordningen, dataskyddslagen och brottsdatalagen. Kamerabevakningslagen kan därför inte träda i kraft förrän samtliga dessa regleringar börjar gälla. Det föreslås därför att lagen ska träda i kraft den 1 augusti 2018. Samtidigt ska kameraövervakningslagen upphöra att gälla. Samma ikraftträdande föreslås i fråga om ändringen i offentlighets- och sekretesslagen.

Befintliga beslut om tillstånd och anmälningar

När kamerabevakningslagen träder i kraft kommer det att finnas ett stort antal tillstånd till kameraövervakning som har beslutats enligt kameraövervakningslagen och som avser sådan kamerabevakning som även omfattas av tillståndskravet enligt den nya lagen. Länsstyrelserna har genom sitt chefsnätverk inkommit med en skrivelse till Justitiedepartementet (Ju 2017/09827/L6) där man lämnar liknande synpunkter som *Datainspektionen* och bl.a. påtalar de praktiska svårigheterna med att avgöra vilka äldre tillstånd som fortfarande ska gälla. Länsstyrelserna föreslår därför att samtliga tillstånd ska upphöra i samband med att den nya lagen träder i kraft.

Att ompröva samtliga befintliga tillståndsbeslut skulle vara förenat med omfattande administration, både för tillsynsmyndigheten och innehavarna av sådana tillstånd. Den prövning som ska göras enligt den nya lagen kommer inte heller att vara strängare än enligt den äldre lagen. Prövningen enligt kamerabevakningslagen innefattar som Datainspektionen framhåller i och för sig en bedömning av om kamerabevakningen är laglig i den mening som krävs enligt framför allt dataskyddsförordningen eller brottsdatalagen. Utgångspunkten är dock att fler tillstånd ska kunna beviljas än tidigare. Det skulle därför inte bidra till integritetsskyddet att ompröva samtliga befintliga tillstånd.

Att låta redan beviljade tillstånd fortsätta att gälla stämmer dessutom väl överens med skäl 171 till dataskyddsförordningen där det framgår att tillstånd från tillsynsmyndigheterna som utfärdats på grundval av det nuvarande dataskyddsdirektivet ska fortsätta att vara giltiga tills de ändras, ersätts eller upphävs. Enligt de riktlinjer som antagits av artikel 29-grupppen ska kravet på konsekvensbedömningen primärt vara tillämpligt på sådana behandlingssituationer som initierats efter att dataskyddsförordningen börjar tillämpas den 25 maj 2018 och på befintliga behandlingar där riskerna av något skäl har ändrats (WP 248 rev.01).

Kamerabevakningslagen bör därför innehålla en övergångsbestämmelse om att tillstånd till kameraövervakning som har beslutats enligt kameraövervakningslagen och som avser kamerabevakning som omfattas av kravet på tillstånd i den nya lagen fortfarande ska gälla. Befintliga tillstånd till kameraövervakning som inte kräver tillstånd enligt den nya lagen bör däremot inte längre gälla. Detta bör av tydlighetsskäl också framgå av en övergångsbestämmelse. Av tydlighetsskäl bör dessutom framgå att anmälningar som har gjorts enligt kameraövervakningslagen inte längre ska gälla.

Befintliga beslut om undantag från upplysningsplikten i enskilda fall

När det gäller beslut enligt kameraövervakningslagen om undantag från upplysningsplikten i enskilda fall kan konstateras att tillsynsmyndigheten också enligt den nya lagen ska ha möjlighet att meddela sådana undantag. En prövning enligt den nya lagen innefattar visserligen också en prövning av förutsättningarna att göra undantag från den rätt till information om den personuppgiftsbehandling som föreligger enligt annan tillämplig personuppgiftsreglering, främst dataskyddsförordningen eller brottsdatalagen. Det nuvarande undantaget innefattar emellertid ett krav på synnerliga skäl och det framgår av både utredningens kartläggning och tidigare lagstiftningsarbete på området att det tillämpas mycket restriktivt. Den befintliga ordningen har bedömts vara förenlig med regleringen i det nuvarande dataskyddsdirektivet som ställer likartade krav i fråga om begränsningar av rätten till information som den nya dataskyddsregleringen. De beslut som har meddelats med stöd av detta undantag i kameraövervakningslagen får därför förutsättas vara förenliga också med den nya EU-regleringen. Beslut om undantag från upplysningsplikten som meddelats med stöd av 27 § tredje stycket kameraövervakningslagen bör därför anses utgöra beslut om undantag från upplysningskravet och rätten till information enligt kamerabevakningslagen.

Pågående ärendehandläggning och överklagade beslut

Den nya lagen innebär bl.a. förbättrade möjligheter att få tillstånd till kamerabevakning som snabbt bör få genomslag i rättstillämpningen. Dessutom måste framtida prövningar och beslut vara förenliga med den nya EU-regleringen. Det är därför lämpligt att ansökningar om tillstånd till kamerabevakning som gjorts enligt den gamla lagen men som inte har hunnit avgöras före den nya lagens ikraftträdande prövas enligt den nya lagen. Detta gäller även för prövning av överklaganden som skett före

ikraftträdandet men som ännu inte har avgjorts. Detsamma bör gälla för ansökningar om undantag från kravet på upplysning och andra frågor enligt kameraövervakningslagen som vid ikraftträdandet av den nya lagen är anhängiggjorda i ärenden hos länsstyrelserna eller som överklagats till allmän förvaltningsdomstol, t.ex. mål som rör föreläggande från tillsynsmyndigheten. Eftersom det följer av allmänna principer att nya bestämmelser gäller från och med att de träder i kraft behövs inga särskilda övergångsbestämmelser om detta.

Vidare är det rimligt att ansökningsärenden hos länsstyrelserna överlämnas till den myndighet som ska pröva ansökningar enligt den nya lagen, dvs. Datainspektionen. Detta bör som utredningen föreslår framgå av en övergångsbestämmelse. Däremot anser regeringen, till skillnad från utredningen, inte att det finns skäl att låta pågående mål i domstol överlämnas till Förvaltningsrätten i Stockholm respektive Kammarrätten i Stockholm. Att mål enligt den nya lagen kommer att koncentreras till dessa domstolar är som framhålls i avsnitt 11.4 en följd av att beslut framöver endast kommer att meddelas av Datainspektionen och bör därför inte föranleda en överflyttning av pågående mål.

Som framgår av avsnitt 11.4 föreslås en särskild bestämmelse i kamerabevakningslagen om att tillsynsmyndigheten, dvs. Datainspektionen, blir motpart när myndighetens beslut överklagas till domstol. Eftersom prövningen av pågående mål bör ske i enlighet med den nya lagen efter ikraftträdandet bör tillsynsmyndigheten enligt den nya lagen ges ställning som motpart i samtliga dessa mål. Som *Kammarrätten i Stockholm* förespråkar bör detta framgå av en övergångsbestämmelse.

I vissa pågående ärenden och mål kommer ändamålet med ansökan eller överklagandet att förfalla med anledning av att den nya lagen träder i kraft. Det handlar exempelvis om ansökningar och överklaganden beträffande tillstånd till sådan kameraövervakning som inte omfattas av den nya lagens tillståndskrav. I sådana fall torde ärendet eller målet oftast kunna avskrivas. Det kan inte uteslutas att vissa andra praktiska frågor kan komma att uppstå hos tillsynsmyndigheten eller domstolarna under en begränsad övergångsperiod. Eftersom sådana frågor bör bli förhållandevis ovanliga och är svåra att förutse bör hanteringen överlämnas åt rättstillämpningen.

Skadestånd

Utredningen föreslår en övergångsbestämmelse som anger att äldre föreskrifter om skadestånd fortfarande ska gälla för skada som har orsakats före ikraftträdandet. Det följer emellertid redan av allmänna grundsatser att ny lagstiftning ska gälla i fråga om skadestånd med anledning av skadefall som inträffar efter ikraftträdandet, medan äldre lag ska tillämpas på skadefall som har inträffat dessförinnan (se prop. 1972:5 s. 593). Regeringen gör därför bedömningen att det inte behövs någon särskild övergångsbestämmelse om detta.

Straffbestämmelsens avskaffande och de nya sanktionsavgifterna

Precis som förslagen till dataskyddslag och brottsdatalag innebär förslaget till kamerabevakningslag att den straffrättsliga regleringen ersätts av ett system med administrativa sanktionsavgifter vid överträdelser. Därmed

uppkommer frågan om vad som ska gälla för straffbelagda gärningar som har begåtts vid kameraövervakning före den nya lagen har trätt i kraft.

Vid bedömningen av behovet att meddela övergångsbestämmelser för den nu nämnda situationen behöver bestämmelserna i såväl 2 kap. 10 § regeringsformen som 5 § andra stycket lagen (1964:163) om införande av brottsbalken beaktas.

I 2 kap. 10 § regeringsformen finns ett förbud mot retroaktiv straff- och skattelagstiftning. Förbudet anses analogivis tillämpligt beträffande straffliknande administrativa påföljder. Att ta ut sanktionsavgifter för överträdelser som begåtts före kamerabevakningslagens ikraftträdande skulle således kunna strida mot retroaktivitetsförbudet. Av 5 § andra stycket lagen om införande av brottsbalken framgår att straff ska bestämmas enligt den lag som gällde när gärningen företogs. Detta är dock inte fallet om annan lag gäller när dom meddelas, under förutsättning att den nya lagen leder till frihet från straff eller till lindrigare straff. Denna bestämmelse har enligt förarbetena generell räckvidd, dvs. den gäller även utanför brottsbalkens tillämpningsområde (se prop. 1964:10 s. 99). Bestämmelsen ger uttryck för den lindrigaste lagens princip.

Bestämmelserna i den nya dataskyddsregleringen innebär att överträdelser överförs från det straffrättsliga området till ett system med enbart administrativa sanktionsavgifter. Formellt sett får sanktionsavgiften anses lindrigare och borde därmed få genomslag bakåt i tiden. Huvudsyftet med den nya dataskyddsregleringens system med kraftfulla sanktionsavgifter är emellertid framför allt att effektivisera sanktionssystemet. Att överträdelser av den nya dataskyddsregleringen, inbegripet kamerabevakningslagen, avkriminaliseras ska inte ses som ett uttryck för att överträdelserna ska bedömas lindrigare än tidigare. Regeringen anser därför att lindrigaste lagens princip inte gör sig särskilt starkt gällande i detta fall. Det finns därför inte skäl att låta systemet med sanktionsavgifter få retroaktiv effekt. Motsvarande bedömning har gjorts i förslagen till dataskyddslag och brottsdatalag. För ett liknande resonemang rörande sanktionsväxling, se propositionen Administrativa sanktioner på yrkesfiskets område, prop. 2007/08:107 och propositionen Effektivare sanktioner för arbetsmiljö- och arbetstidsreglerna, prop. 2012/13:143 s. 82. Äldre föreskrifter om straff bör alltså tillämpas på överträdelser som skett före kamerabevakningslagens ikraftträdande.

Offentlighets- och sekretesslagen

När det slutligen gäller ändringen i offentlighets- och sekretesslagen bör den nya lagen innehålla en övergångsbestämmelse om att äldre föreskrifter fortfarande ska gälla för uppgifter som har inhämtats före ikraftträdandet.

13 Konsekvenser av förslagen

13.1 Ekonomiska konsekvenser för det allmänna

Regeringens bedömning: Förslaget innebär ökade kostnader för den myndighet som ska utöva tillsyn enligt kamerabevakningslagen (Datainspektionen) och minskade kostnader för länsstyrelserna. Finansieringen av Datainspektionens behov av ökade anslag bör delvis ske genom en minskning av anslagen till länsstyrelserna.

Förslagen förväntas inte leda till några kostnadsökningar för andra statliga myndigheter eller för landstingen. Förslagen väntas leda till något minskade kostnader för kommunerna.

Utredningens bedömning: Överensstämmer delvis med regeringens. Utredningen bedömer att de ökade kostnaderna för den myndighet som ska utöva tillsyn enligt kamerabevakningslagen är lägre än motsvarande tolv årsarbetskrafter och att dessa delvis kan finansieras genom avgifter. Utredningen bedömer även att förslagen medför ökade kostnader för Förvaltningsrätten i Stockholm och Kammarrätten i Stockholm och att dessa bör finansieras genom att anslagen till övriga förvaltningsrätter och kammarrätter minskar i motsvarande mån. Utredningen bedömer vidare att förslagen väntas medför mindre kostnader av engångskaraktär för kommuner och landsting som ryms inom befintliga ramar.

Remissinstanserna: *Datainspektionen* anser att utredningen har gjort en felaktig uppskattning av myndighetens personella behov som ensam tillsyns- och tillståndsmyndighet för all kamerabevakning i Sverige. Enligt Datainspektionens bedömning behöver myndigheten uppskattningsvis 50 årsarbetskrafter, eller ca 65 miljoner kronor per år för sina föreslagna uppgifter på området för kamerabevakning. Detta inkluderar resekostnader, kostnader för information m.m. *Länsstyrelsen i Dalarna* och *Länsstyrelsen Gävleborg* anför att det saknas utredning om vilka konsekvenser en minskning av anslagen kan tänkas få för länsstyrelserna. Enligt *Förvaltningsrätten i Jönköping* har de flesta medelstora förvaltningsrätter så få mål av den aktuella måltypen att det inte är möjligt att särskilja kostnaderna för dessa mål.

Regeringens förslag och bedömning

Datainspektionen och länsstyrelserna

Den myndighet som regeringen bestämmer ska vara ensam tillsynsmyndighet enligt kamerabevakningslagen. Enligt regeringens bedömning bör denna myndighet vara Datainspektionen (se avsnitt 11.1). Det innebär att Datainspektionen, utöver det tillsynsansvar som inspektionen har i dag på kameraområdet, får nya uppgifter i form av tillståndsprövning och operativ tillsynen över kamerabevakning av platser dit allmänheten har tillträde. Datainspektionen ska också pröva ansökningar som rör undantag i enskilda fall från upplysningskravet och enskildas rätt till information om den personuppgiftsbehandling som kamerabevakningen innebär.

Samtidigt som Datainspektionen får nya uppgifter kommer länsstyrelserna att upphöra med de uppgifter som de har haft enligt kameraövervakningslagen. Förslaget innebär därför ökade kostnader för Datainspektionen och minskade kostnader för länsstyrelserna. Enligt utredningens kartläggning uppgick den totala resursåtgången avseende kameraövervakning för landets 21 länsstyrelser under år 2015 till omkring tolv årsarbetskrafter. Utredningen uppskattar att 10–15 procent av den totala arbetsinsatsen vid länsstyrelserna i dag avser faktisk tillsyn, vilket innebär att resurserna huvudsakligen används för handläggning av tillståndsärenden och hanteringen av anmälningar. Enligt uppgifter från länsstyrelserna avgjordes drygt 900 ärenden om tillstånd under 2015 samtidigt som antalet anmälningar uppskattas uppgå till drygt 1000 stycken per år.

Länsstyrelsernas verksamhet på det aktuella området är i dag delvis finansierad genom avgifter. Utredningen uppskattar att avgifterna för år 2015 motsvarade en inkomst på cirka fyra miljoner kronor och att, om avgiftsfinansieringen skulle finnas kvar i den nya lagen, denna inkomst skulle minska till omkring 1,5–2,2 miljoner kronor. Till skillnad från utredningen föreslår regeringen emellertid ingen föreskriftsrätt angående avgifter för ansökningar enligt den nya lagen (se avsnitt 11.5).

Kamerabevakningslagen kommer att ha ett snävare tillämpningsområde och ett mer begränsat tillståndskrav än kameraövervakningslagen. Den nya lagen kommer inte heller innehålla något anmälningsförfarande för viss kamerabevakning. För tillsynsmyndighetens del kommer förslagen alltså att leda till betydligt färre tillståndsprocesser och att hanteringen av anmälningar helt försvinner. En större andel av tillsynsmyndighetens resurser bör därmed kunna koncentreras till bl.a. information, vägledning och egentlig tillsynsverksamhet.

Datainspektionen utövar redan i dag tillsyn över kameraövervakning av platser dit allmänheten inte har tillträde. I enlighet med vad utredningen anför kan Datainspektionens tillkommande tillsynsansvar också samordnas med myndighetens tillsyn av personuppgiftsbehandling i stort, vilket kan väntas medföra vissa effektivitetsvinster. Datainspektionen kommer inte heller ha kvar någon samordnande roll i förhållande till länsstyrelserna eller behov av att hämta in och analysera beslut från länsstyrelserna.

Utredningen bedömer att resurstillskottet till Datainspektionen, med hänsyn bl.a. till nämnda effektivitetsvinster, bör vara lägre än de motsvarande tolv årsarbetskrafter som i dag finns vid länsstyrelserna. Som *Datainspektionen* anför kommer tillsynen enligt den nya kamerabevakningslagen emellertid att vara av en annan karaktär än den som bedrivs enligt kameraövervakningslagen. Detta beror framför allt på att en betydande del av tillsynen kommer bestå av prövningar av kamerabevakningens laglighet i förhållande till regleringen i dataskyddsförordningen och brottsdatalagen. Med anledning av att tekniken blir mer tillgänglig och tillståndskravet inte längre kommer omfatta den privata sektorn kan kamerabevakningen i samhället dessutom förväntas öka.

EU:s nya dataskyddsreglering innebär vidare att tillsynsmyndigheten får fler uppgifter än tidigare och utökade befogenheter. Både dataskyddsförordningen och det nya dataskyddsdirektivet innehåller krav

på att varje medlemsstat ska säkerställa att tillsynsmyndigheten förfogar över bl.a. 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.

Finansiering av Datainspektionens behov bör i enlighet med utredningens bedömning delvis ske genom en minskning av anslagen till länsstyrelserna. Det är samtidigt angeläget att tillsynen på området förstärks. Regeringen bedömer att kostnaderna för Datainspektionens tillkommande uppgifter och tillsyn enligt kamerabevakningslagen uppgår till ca 20 miljoner kronor.

Domstolarna

Enligt utredningens kartläggning överklagades under år 2015 knappt 130 beslut om tillstånd till kameraövervakning. I och med att tillståndskravet enligt den nya lagen blir mer begränsat kan antalet överklagade tillståndsbeslut till allmän förvaltningsdomstol förväntas minska. Datainspektionen kommer enligt den nya lagen att pröva sådana ansökningar som första instans vilket innebär att det huvudsakligen är den som vill bedriva kamerabevakning som kommer att ha anledning att överklaga besluten. Eftersom möjligheterna att få tillstånd också förbättras kan antalet ärenden som överklagas till domstol väntas bli förhållandevis få.

Även beslut och överklaganden som rör undantag från upplysningskravet i enskilda fall väntas bli relativt sällsynta. Detsamma gäller beslut från tillsynsmyndigheten om administrativa sanktionsavgifter för överträdelser av bestämmelser i kamerabevakningslagen, liksom domstolsprövningar av sådana beslut. Sådana processer ersätter dessutom dagens ordning med straffansvar och talan om brott. Sammanfattningsvis väntas förslagen därför inte leda till några ökade kostnader för Sveriges Domstolar.

Att Datainspektionen blir ensam tillsynsmyndighet enligt kamerabevakningslagen innebär att de beslut som överklagas kommer att koncentreras till Förvaltningsrätten i Stockholm och Kammarrätten i Stockholm. Samtidigt som antalet överklaganden väntas minska generellt kan det alltså komma att ske en viss ökning av antalet mål i dessa båda domstolar. Det ingår i Domstolsverkets uppgifter att åstadkomma en ändamålsenlig resursfördelning mellan domstolarna.

Andra statliga myndigheter, kommuner och landsting

Förslagen väntas inte leda till några kostnadsökningar för andra statliga myndigheter än vad som redovisas ovan. De myndigheter som bedriver kamerabevakning kan i och för sig behöva göra vissa nya typer av överväganden men det måste främst betraktas som en konsekvens av kraven i den EU-rättsliga dataskyddsregleringen.

Att myndigheter ska kunna påföras sanktionsavgifter vid överträdelser av bestämmelser i kamerabevakningslagen skulle kunna orsaka ökade kostnader i enskilda fall. Beslut om sanktionsavgifter mot myndigheter förväntas dock bli sällsynta. Det beror framför allt på att myndigheter förväntas anpassa verksamheten efter tillsynsmyndighetens synpunkter utan att det krävs sådana repressiva åtgärder.

Med anledning av att regeringen utformar förlagen om upplysningskrav vid kamerabevakning och förhandlingsskyldighet vid kamerabevakning på arbetsplatser delvis annorlunda än utredningen väntas förslagen inte heller innebära några kostnadsökningar av engångskaraktär för kommunerna eller landstingen. Kamerabevakningslagens snävare tillämpningsområde, det begränsade tillståndskravet och det faktum att kommunerna bara ska ges tillfälle att yttra sig i ärenden om det av särskild anledning behövs ett yttrande kan snarare väntas leda till något minskade kostnader för kommunerna.

13.2 Ekonomiska konsekvenser för enskilda

Regeringens bedömning: Förslagen förväntas leda till minskade kostnader och en minskad administrativ börda för den stora merparten av de enskilda som bedriver kamerabevakning.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Visita* anser att utredningen inte fullt ut har beaktat vissa faktorer som kan få konsekvenser för enskilda som använder kamerabevakning. Utredningen gör enligt Visita t.ex. inte någon bedömning av i vilken utsträckning företagen kommer att behöva göra konsekvensbedömningar och samråda med tillsynsmyndigheten i enlighet med regleringen i dataskyddsförordningen och uppskattar inte heller vad detta kan komma att innebära för företagen i tid, administration eller kostnader. Enligt Visita saknas också en bedömning av riskerna för att företagen drabbas av omfattande sanktionsavgifter samt processkostnader i de fall där tillsynsmyndigheten gör andra bedömningar än företagen.

Regeringens bedömning: Förslagen innebär att det i stor utsträckning inte längre kommer att krävas tillstånd eller anmälan för att enskilda ska få bedriva kamerabevakning. I dessa fall kommer förslagen att medföra en kostnadsminskning för de enskilda eftersom de inte behöver betala avgifter för att få bedriva bevakningen eller lägga tid på ett ansöknings- eller anmälningsförfarande. Som utredningen anför kan förslagen också innebära förbättrade konkurrensförutsättningar för svenska företag eftersom regleringen blir mer lik vad som gäller i andra EU-länder.

Enskilda som inte längre omfattas av krav på tillstånd eller anmälan för att använda kamerabevakning måste alltjämt förhålla sig till de krav och skyldigheter som framgår av dataskyddsförordningen. Detta innebär bl.a. att de måste göra en avvägning mellan det egna intresset av kamerabevakning på platsen och de registrerades intresse av skydd för den personliga integriteten. Detta innebär också, som *Visita* framhåller, att enskilda i vissa fall kan behöva göra en konsekvensbedömning och även samråda med tillsynsmyndigheten i enlighet med regleringen i dataskyddsförordningen. Vid överträdelser kommer också förordningens administrativa sanktionsavgifter att gälla. Detta är emellertid en direkt konsekvens av att dataskyddsförordningen är tillämplig på sådan personuppgiftsbehandling som sker vid kamerabevakning och inte en konsekvens av förslagen i detta lagstiftningsärende. Det kan i detta sammanhang nämnas att Datainspektionen har fått i uppdrag av regeringen att ta fram stöd för näringslivets anpassning till dataskyddsförordningen

(2016-11-24, N2016/07306/FÖF). Vidare finns möjlighet för branschorganisationer att utarbeta uppförandekoder med inriktning på den aktuella branschen som stöd för de enskilda medlemsföretagens verksamhet med kamerabevakning (artikel 40 i dataskyddsförordningen).

13.3 Konsekvenser för det brottsförebyggande arbetet och brottsligheten

Regeringens bedömning: Förslagen väntas ge positiva effekter för det brottsförebyggande arbetet och för motverkandet av brottslighet i övrigt.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt i frågan.

Skälen för regeringens bedömning: Kamerabevakning är ett verktyg bland flera som kan hjälpa till att förebygga, förhindra eller upptäcka brottslighet och bidra till att begångna brott kan utredas och lagföras. Undersökningar, både svenska och utländska, visar att kamerabevakning har vissa brottsförebyggande effekter. Vidare kan realtidstillgång till material från kamerabevakning vara av stort värde för Polismyndighetens operativa brottsförebyggande insatser. Bild- och ljudmaterial från kamera-bevakning, både från Polismyndighetens egen bevakning och från andra aktörers bevakning, används dessutom ofta i brottsutredningar på ett sätt som kan föra utredningarna framåt och bidra till att lagföring sker.

Förslagen innebär som helhet att möjligheterna att bedriva kamerabevakning ökar, inte minst när bevakningen ska ske för brottsbekämpande ändamål. Kamerabevakning kommer i större utsträckning att få ske utan tillstånd och i de fall tillstånd krävs kommer det att bli lättare att få tillstånd. Dessa ökade möjligheter att bedriva kamerabevakning väntas ge positiva effekter för det brottsförebyggande arbetet. De bedöms också ge positiva effekter för motverkandet av brottslighet i övrigt, eftersom material från kamerabevakning i större utsträckning kommer att användas för utredning och lagföring av brott. Att begångna brott utreds och lagförs kan vidare bidra till att straffsystemet får avsedd generell brottsavhållande verkan.

13.4 Konsekvenser för skyddet av den personliga integriteten och övriga konsekvenser

Regeringens bedömning: Förslagen innebär ett förstärkt skydd för enskildas personliga integritet och kan på sikt förbättra möjligheterna att nå de integrations- och jämställdhetspolitiska målen.

Förslagen förväntas inte få några konsekvenser för den kommunala självstyrelsen.

Utredningens bedömning överensstämmer i huvudsak med regeringens. Utredningen bedömer dock att förslagen inte väntas få några

konsekvenser för jämställdheten eller för möjligheterna att nå de integrationspolitiska målen.

Remissinstanserna: *Länsstyrelsen i Dalarna* delar bedömningen att minskad brottslighet kan innebära en förbättring av integritetsskyddet. Länsstyrelsen anser också att utredningens förslag till förstärkningar av skyddet för den personliga integriteten är ändamålsenliga och väl avvägda. Däremot anser länsstyrelsen att riskerna för den personliga integriteten kan komma att öka om tillsynen över kamerabevakning kommer att minska i omfattning. *Länsstyrelsen i Östergötlands län* anser att det är oklart om utredningens förslag innebär att Datainspektionen tilldelas tillräckliga resurser för att kunna bedriva en effektiv tillsyn i hela landet. I sådana fall skulle förslagen enligt länsstyrelsen inte innebära ett förstärkt skydd för den personliga integriteten.

Skälen för regeringens bedömning: Kamerabevakning innebär typiskt sett ett intrång i rätten till skydd för den personliga integriteten. Ökade möjligheter att bedriva kamerabevakning kan därför medföra högre risker för den personliga integriteten. Att bli utsatt för brott kan emellertid också utgöra en kränkning av den personliga integriteten. I den mån de ökade möjligheterna att bedriva kamerabevakning leder till minskad brottslighet kan därför en förbättring av integritetsskyddet uppnås.

Dessutom föreslås flera förstärkningar av integritetsskyddet vid kamerabevakning. En av dessa är att det görs tydligt att bestämmelserna om förhandlingsskyldighet i lagen om medbestämmande i arbetslivet kan vara tillämpliga inför beslut om kamerabevakning på arbetsplatser. Detta förväntas öka efterlevnaden av både regleringen i kamerabevakningslagen och lagen om medbestämmande i arbetslivet. Ett annat förslag som bedöms innebära ett förbättrat integritetsskydd är att tillsynen på området samlas hos en myndighet, Datainspektionen, som dessutom får fler uppgifter och utökade befogenheter med anledning av EU:s nya dataskyddsreglering. Genom regeringens budgetproposition för 2018 (prop. 2017/18:1) har Datainspektionens anslag ökats med 30 miljoner kronor från år 2018 för myndighetens tillkommande arbetsuppgifter med anledning av dataskyddsförordningen. Regeringen anser dessutom, som framgår av avsnitt 13.1, att tillsynen på kamerabevakningsområdet bör förstärkas genom att Datainspektionen tillförs mer resurser. Skyddet för enskildas personliga integritet kommer också förstärkas genom att EU-regleringens detaljerade bestämmelser om bl.a. rättigheter för registrerade och skyldigheter för personuppgiftsansvariga samt system med administrativa sanktionsavgifter kommer att gälla även vid kamerabevakning.

Förslagen innebär förbättrade möjligheter att använda kamerabevakning i utsatta områden vilket kan bidra till ökad trygghet i sådana områden och på sikt förbättra möjligheterna att nå de integrationspolitiska målen. De förbättrade möjligheterna att använda kamerabevakning för brottsbekämpande och trygghetsskapande syften kan på sikt också bidra till mer jämställda villkor i samhället och att uppnå det jämställdhetspolitiska målet om att mäns våld mot kvinnor ska upphöra.

Förslagen förväntas inte få några konsekvenser för den kommunala självstyrelsen.

14 Författningskommentar

14.1 Förslaget till kamerabevakningslag

Allmänna bestämmelser

1 § I denna lag finns bestämmelser om kamerabevakning som

– kompletterar Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), här benämnd EU:s dataskyddsförordning, och

– genomför 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, här benämnt EU:s dataskyddsdirektiv.

I lagen finns också bestämmelser om sådan kamerabevakning som inte omfattas av EU:s dataskyddsförordning eller EU:s dataskyddsdirektiv.

Paragrafen anger lagens innehåll. Övervägandena finns i avsnitt 5.1.

I paragrafen anges att lagen innehåller bestämmelser om kamerabevakning som kompletterar EU:s dataskyddsförordning, bestämmelser om kamerabevakning som genomför EU:s dataskyddsdirektiv och bestämmelser som avser sådan kamerabevakning som inte omfattas av dataskyddsförordningen eller dataskyddsdirektivet. Hänvisningen till dataskyddsförordningen avser förordningen i den vid varje tidpunkt gällande lydelsen.

Lagens syfte

2 § Syftet med denna lag är att tillgodose behovet av kamerabevakning för berättigade ändamål och att skydda fysiska personer mot otillbörligt intrång i den personliga integriteten vid sådan bevakning.

Paragrafen, som motsvarar 1 § kameraövervakningslagen, anger lagens syfte. Övervägandena finns i avsnitt 5.3.1.

I bestämmelsen anges att lagens syfte är dels att tillgodose behovet av kamerabevakning för berättigade ändamål, dels att skydda fysiska personer mot otillbörligt intrång i den personliga integriteten vid kamerabevakning. Avsikten med lagen är alltså att reglera kamerabevakning på ett sätt som innebär en lämplig balans mellan nyttan med kamerabevakning och skyddet av den personliga integriteten.

Med berättigade ändamål avses både sådana ändamål som ska beaktas särskilt vid tillståndsprövningen enligt 8 § och andra ändamål som betraktas som berättigade i enlighet med de regleringar om behandling av personuppgifter som avses i 6 §.

Kamerabevakning

3 § Med kamerabevakning avses

1. att en tv-kamera, ett annat optisk-elektroniskt instrument eller en därmed jämförbar utrustning, utan att manövreras på platsen, används på ett sätt som innebär varaktig eller regelbundet upprepad personbevakning,
2. att en separat teknisk anordning för avlyssning eller upptagning av ljud används i samband med sådan användning av utrustning som avses i 1, eller
3. att en separat teknisk anordning används för att behandla bild- och ljudmaterial som tagits upp med sådan utrustning som avses i 1 eller 2.

Paragrafen, som delvis motsvarar 2 och 3 §§ kameraövervakningslagen, innehåller en definition av begreppet kamerabevakning. Övervägandena finns i avsnitt 5.3.3.

Enligt *punkten 1* avses med kamerabevakning att en tv-kamera, ett annat optisk-elektroniskt instrument eller en därmed jämförbar utrustning, utan att manövreras på platsen, används på ett sätt som innebär varaktig eller regelbundet upprepad personbevakning.

Den utrustning som omfattas – tv-kameror, andra optisk-elektroniska instrument och därmed jämförbara utrustningar – är densamma som omfattas av hittillsvarande kameraövervakningslag. Därmed omfattas i princip alla typer av kameror där bildupptagningen förmedlas vidare till en elektronisk bildskärm eller lagras på ett elektroniskt medium. Med därmed jämförbar utrustning avses t.ex. instrument som kan nyttja sådan elektromagnetisk strålning som röntgen och radiofrekvent strålning.

Även uttrycket utan att manövreras på platsen har samma innebörd som i kameraövervakningslagen. Med platsen menas den plats där utrustningen finns. Utrustningen kan finnas antingen på en fast plats, t.ex. på en fasad, på en inomhusvägg, i ett tak eller på en stolpe, eller på en rörlig plats, t.ex. på eller i ett fordon, ett fartyg eller en drönare eller ett annat luftfartyg. Med att utrustningen används utan att manövreras på platsen avses att den fortlöpande hanteringen av utrustningen sker på ett ställe som är klart åtskilt från den plats där utrustningen finns. Endast det förhållandet att utrustningen sätts igång på stället eller fungerar med inbyggd automatik innebär inte att den manövreras på platsen.

Utrustning som finns i användarens omedelbara närhet och som fortlöpande styrs av användaren är manövrerad på platsen. Lagen omfattar därför inte handhållna kameror eller annan därmed jämförbar utrustning och inte heller kameror som på annat sätt är kroppsburna, t.ex. en kamera som är fäst i en persons kläder eller monterad på en hjälm. Lagen omfattar normalt inte heller användning av exempelvis en webbkamera, utrustning för videokonferens, en kamera placerad på vindrutan i en bil eller en kamera fäst på ett cykelstyre förutsatt att användaren är i kamerans eller utrustningens omedelbara närhet och fortlöpande styr över denna, dvs. avgör att den ska användas och vad som ska fotograferas eller filmas.

För att det ska vara fråga om kamerabevakning enligt punkten 1 krävs dessutom att utrustningen används på ett sätt som innebär varaktig eller regelbundet upprepad personbevakning. Begreppet personbevakning har samma innebörd som begreppet personövervakning i kameraövervakningslagen. Med personbevakning avses således att personer kan identifieras genom bevakningen. Det krävs att sådana kännetecken kan iakttas som gör att man utan större osäkerhet kan skilja

de personer som iakttas från andra personer. Så är fallet om hela personen eller personens ansikte syns tydligt. Även sådant som utmärkande klädsel, speciella kroppsrörelser eller särskild kroppskonstitution kan möjliggöra identifiering.

Med varaktig personbevakning avses t.ex. bevakning med en kamera som under en längre tid är placerad på eller riktad mot en plats där människor normalt vistas. Bevakning med en kamera som är placerad på ett torg, i en butik, i ett väntrum eller i en buss, är därmed normalt att bedöma som sådan varaktig personbevakning som gör att lagen är tillämplig.

Med regelbundet upprepad personbevakning menas personbevakning vid ett flertal tillfällen. I kravet på regelbundenhet ligger att det i första hand ska vara fråga om tillfällen som ligger relativt nära varandra i tiden. Även bevakning vid tillfällen som är mer utspridda kan emellertid betraktas som regelbunden om det är fråga om systematisk användning av bevakningsutrustning. Därmed omfattas exempelvis sådana rörliga kameror som är monterade på en drönare av lagens tillämpningsområde, om användningen innebär att människor ofta passerar i kamerans upptagningsområde på ett sätt som gör dem möjliga att identifiera. På samma sätt omfattas kameror som riktas ut från ett fordon, så länge kameran inte kan anses vara manövrerad på platsen. Även utplacering och användning av kameror på platser där människor passerar mer sällan men med viss regelbundenhet, exempelvis i närheten av en gångstig i skogen, omfattas av lagens tillämpningsområde.

Om kameran används på ett sätt som endast innebär enstaka fall av helt kortvarig personbevakning är lagen dock inte tillämplig. Så kan t.ex. vara fallet med kameror som används på svårtillgängliga platser i utomhusmiljöer eller som placeras för att kontrollera en industriell tillverkningsprocess i vars närhet människor normalt inte ska befinna sig, även om någon vid ett enstaka tillfälle kan råka göra det. Detta innebär också att den som använder en kamerautrustad drönare har möjlighet att se till att lagen inte blir tillämplig genom att personer vare sig varaktigt eller regelbundet upprepat fångas av kameran på ett sätt som gör dem möjliga att identifiera. Detta kan exempelvis åstadkommas genom att kameran bara är påslagen på en viss höjd eller stängs av när människor som går att identifiera kommer in i kamerans upptagningsområde.

Syftet med användningen av kamerautrustningen saknar betydelse för frågan om lagens tillämplighet. Lagen är tillämplig både vid sådan användning av kameror som sker i syfte att bevaka människor och sådan användning som sker för andra syften men där människor samtidigt under en längre tid eller någorlunda regelbundet kommer in i kamerans upptagningsområde på ett sätt som gör dem möjliga att identifiera.

Av *punkten 2* framgår att med kamerabevakning avses även att en separat teknisk anordning för avlyssning eller upptagning av ljud används i samband med användning av sådan utrustning som avses i punkten 1. Exempel på sådana anordningar är mikrofoner och radiosändare som inte är inbyggda i utrustning som omfattas av punkten 1.

Slutligen framgår av *punkten 3* att med kamerabevakning avses också att en separat teknisk anordning för att behandla upptaget bild- och ljudmaterial används. Exempelvis avses användning av separata anordningar för att lagra inspelad film.

Lagens tillämpningsområde

4 § Lagen gäller endast om

1. kamerabevakning enligt 3 § 1 eller 2 sker med utrustning som finns i Sverige och den som bedriver bevakningen är etablerad i Sverige eller i tredjeland, eller
2. kamerabevakning enligt 3 § 3 avser behandling av bild- och ljudmaterial som tagits upp vid bevakning som avses i 1 och behandlingen utförs av den som bedriver bevakningen eller för hans eller hennes räkning.

I paragrafen, som i huvudsak motsvarar 3 § kameraövervakningslagen, finns bestämmelser om lagens territoriella tillämpningsområde. Övervägandena finns i avsnitt 5.3.4.

Av *punkten 1* framgår att kamerabevakningslagen endast är tillämplig på sådan kamerabevakning som avses i 3 § 1 eller 2, om utrustningen finns i Sverige och den som bedriver bevakningen är etablerad i Sverige eller i tredjeland. Med Sverige avses svenskt landterritorium och sjöterritorium samt luftrummet ovanför land- och sjöterritorierna. Lagen är alltså inte tillämplig vid kamerabevakning på svenska ambassader eller liknande platser utanför Sveriges gränser. Begreppet tredjeland ska tolkas på samma sätt som i dataskyddsförordningen och dataskyddsdirektivet.

Av *punkten 2* följer att lagen även är tillämplig vid sådan efterföljande behandling som anses utgöra kamerabevakning enligt 3 § 3, om behandlingen avser bild- och ljudmaterial som tagits upp vid bevakning enligt punkten 1 och behandlingen utförs av den som bedriver bevakningen eller för hans eller hennes räkning. Lagen gäller däremot inte om materialet överlämnas till någon annan som därigenom övertar personuppgiftsansvaret för behandlingen.

5 § Lagen gäller inte vid

1. kamerabevakning som en fysisk person utför som ett led i en verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll,
2. hemlig kameraövervakning enligt 27 kap. rättegångsbalken eller lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott,
3. kamerabevakning som sker i en verksamhet som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen, eller
4. kamerabevakning som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

I paragrafen finns bestämmelser om undantag från lagens tillämpningsområde. Punkten 1 motsvarar 5 § kameraövervakningslagen och punkten 2 motsvarar 4 § kameraövervakningslagen, medan punkterna 3 och 4 saknar motsvarighet i den lagen. Övervägandena finns i avsnitt 5.3.5.

Enligt *punkten 1* gäller lagen inte vid kamerabevakning som en fysisk person utför som ett led i en verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll. Undantagets lydelse är densamma som artikel 2.2 c i dataskyddsförordningen. Undantaget omfattar endast kamerabevakning som bedrivs av fysiska personer, inte bevakning som utförs av juridiska personer. Kamerabevakning som bedrivs på uppdrag av en fysisk person, t.ex. av ett bevakningsbolag, kan dock omfattas av undantaget. Den viktigaste faktorn för att avgöra om undantaget är tillämpligt är platsen för kamerabevakningen. Bevakning som sker i en privatbostad av den som bor där omfattas normalt av undantaget.

Detsamma gäller t.ex. bevakning av personens tomtmark, garage och förråd. Undantaget omfattar dock inte kamerabevakning i offentliga miljöer eller av områden som är privatägda men allemansrättsligt tillgängliga, dvs. platser dit allmänheten har tillträde. Undantaget omfattar inte heller kamerabevakning som bedrivs inom ramen för näringsverksamhet, oavsett platsen för bevakningen.

I *punkten 2* undantas hemlig kameraövervakning enligt 27 kap. rättegångsbalken eller lagen om åtgärder för att förhindra vissa särskilt allvarliga brott från lagens tillämpningsområde.

Av *punkten 3* följer att lagen inte omfattar kamerabevakning som sker i en verksamhet som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Undantaget omfattar endast kamerabevakning som sker inom ramen för verksamhet som skyddas genom tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Som exempel kan nämnas direktsändning av ett sportevenemang med kameror uppsatta på drönare. Däremot är undantaget inte tillämpligt om t.ex. en medieredaktion bedriver kamerabevakning utanför den grundlagsreglerade verksamheten, t.ex. för att skydda sina lokaler eller anställda. Vid sådan kamerabevakning är således lagen tillämplig.

Av *punkten 4* följer att lagen inte heller omfattar kamerabevakning som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande utanför det grundlagsskyddade området. Innebörden av begreppen journalistiska ändamål respektive akademiskt, konstnärligt eller litterärt skapande ska i första hand avgöras genom en tolkning av dataskyddsförordningen (artikel 85). Ledning bör dock kunna hämtas från tidigare praxis angående 7 § andra stycket personuppgiftslagen (1998:204).

Lagens förhållande till annan dataskyddsreglering

6 § Utöver vad som föreskrivs i denna lag gäller

1. EU:s dataskyddsförordning, lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning, föreskrifter som har meddelats i anslutning till den lagen och andra föreskrifter som kompletterar dataskyddsförordningen,
2. brottsdatalagen (2018:000), föreskrifter som har meddelats i anslutning till den lagen och andra föreskrifter som genomför EU:s dataskyddsdirektiv, och
3. föreskrifter om sådan behandling av personuppgifter som inte omfattas av dataskyddsförordningens eller brottsdatalagens tillämpningsområde.

Paragrafen anger hur lagens bestämmelser förhåller sig till andra regleringar med bestämmelser om personuppgiftsbehandling. Övervägandena finns i avsnitt 5.3.2.

Av paragrafen framgår att utöver vad som föreskrivs i lagen gäller i tillämpliga delar bestämmelser i annan personuppgiftsreglering. Regleringen i kamerabevakningslagen får ställning som lex specialis i förhållande till annan nationell personuppgiftsreglering. De bestämmelser i andra regelverk som gäller vid kamerabevakning enligt denna paragraf avser sådant som inte är reglerat i kamerabevakningslagen, exempelvis kraven på laglig behandling av personuppgifter, lagringstid och andra allmänna principer för behandling av personuppgifter, skyldigheter för

personuppgiftsansvariga och personuppgiftsbiträden samt rättigheter för registrerade.

I enlighet med *punkten 1* gäller, utöver vad som föreskrivs i denna lag, även dataskyddsförordningen, dataskyddslagen, föreskrifter som har meddelats i anslutning till den lagen eller annan författning som kompletterar dataskyddsförordningen. Hänvisningen till dataskyddsförordningen avser förordningen i den vid varje tidpunkt gällande lydelsen. Att dataskyddsförordningens bestämmelser gäller följer direkt av unionsrätten men anges för att göra paragrafen fullständig och begriplig. Normalt är det bestämmelserna i dataskyddsförordningen och den generella kompletterande regleringen i dataskyddslagen som är tillämpliga. I den mån det i annan författning som kompletterar dataskyddsförordningen, exempelvis i s.k. särskilda registerförfattningar, finns bestämmelser som kan tillämpas på kamerabevakning gäller dock även dessa.

I *punkten 2* anges att i fråga om sådan kamerabevakning som omfattas av EU:s dataskyddsdirektiv gäller brottsdatalagen, föreskrifter som har meddelats i anslutning till den lagen eller annan författning som genomför direktivet.

I *punkten 3* anges att i fråga om sådan kamerabevakning som utgör personuppgiftsbehandling som inte omfattas av dataskyddsförordningens eller brottsdatalagens tillämpningsområde, gäller föreskrifter om personuppgiftsbehandling på detta område. Vad som avses är personuppgiftsbehandling inom områden som inte omfattas av unionsrätten, t.ex. nationell säkerhet, eller omfattas av avdelning V kapitel 2 i EU-fördraget, dvs. den gemensamma utrikes- och säkerhetspolitiken.

Tillstånd till kamerabevakning

Krav på tillstånd

7 § Tillstånd till kamerabevakning av en plats dit allmänheten har tillträde krävs, om bevakningen ska bedrivas av
1. en myndighet, eller
2. någon annan än en myndighet vid utförande av en uppgift av allmänt intresse som följer av lag eller annan författning, kollektivavtal eller beslut som meddelats med stöd av lag eller annan författning.

Paragrafen anger i vilka fall det krävs tillstånd till kamerabevakning. Paragrafen motsvarar delvis 8 § kameraövervakningslagen. Övervägandena finns i avsnitt 6.2.

Av paragrafen följer att tillstånd krävs till kamerabevakning av en plats dit allmänheten har tillträde om bevakningen ska bedrivas av en myndighet. Tillstånd krävs även om sådan bevakning ska bedrivas av någon annan än en myndighet vid utförande av en uppgift av allmänt intresse som följer av lag eller annan författning, kollektivavtal eller beslut som meddelats med stöd av lag eller annan författning.

Med plats dit allmänheten har tillträde menas detsamma som enligt kameraövervakningslagen. Tidigare praxis på området är därför vägledande. Exempelvis avses gator, torg och parker samt transportmedel för allmänna kommunikationer och ankomst- och avgångshallar för

passagerare som använder sådana transportmedel. Ytterligare exempel är utrymmen för allmänheten hos myndigheter, på vårdinrättningar och i simhallar.

Tillståndskravet för kamerabevakning gäller enligt *punkten 1* för alla myndigheter, oavsett vilken typ av verksamhet kamerabevakningen används i och vad syftet med den är. Med myndigheter avses samtliga statliga och kommunala organ, med undantag för riksdagen och kommun- och landstingsfullmäktige. Kommunala och statliga bolag är inte myndigheter även om de utövar offentlig makt.

Enligt *punkten* 2 gäller tillståndskravet också för andra än myndigheter vid utförande av uppgifter av allmänt intresse, förutsatt att uppgiften följer av lag eller annan författning, kollektivavtal eller beslut som meddelats med stöd av lag eller annan författning. Bestämmelsen är i denna del utformad i nära anslutning till 2 kap. 2 § 1 dataskyddslagen som anger förutsättningarna för när ett allmänt intresse kan utgöra en rättslig grund för behandling av personuppgifter enligt dataskyddsförordningen.

Begreppet allmänt intresse är unionsrättsligt men vid tolkningen kan ledning sökas i hur begreppet ska förstås enligt annan svensk lagstiftning. Uppgiften av allmänt intresse ska dessutom vara fastställd på det sätt som anges i paragrafen för att kravet på tillstånd ska gälla.

Bestämmelsen innebär att tillståndskravet omfattar samtliga fall där enskilda subjekt har anförtrotts förvaltningsuppgifter som innebär myndighetsutövning, uppgifter inom brottsdatalagens tillämpningsområde eller uppgifter på området för nationell säkerhet. Kravet på tillstånd gäller också generellt inom hälso- och sjukvård, förutsatt att det rör sig om bevakning av utrymmen som allmänheten har tillträde till. Tillståndskravet omfattar även kamerabevakning av skolområden dit allmänheten har tillträde liksom kollektivtrafik, järnväg, flyg och liknande, förutsatt att den som bedriver verksamheten kan anses utföra en uppgift av allmänt intresse som är fastställd på det sätt som anges i bestämmelsen.

Däremot krävs inte tillstånd vid kamerabevakning i en verksamhet som inte utgör en uppgift av allmänt intresse i den mening som avses i punkten 2. Detta innebär att det i normalfallet inte behövs tillstånd vid kamerabevakning av t.ex. butiker, köpcentrum, restauranger, hotell eller banklokaler. Vidare behövs inte tillstånd när religiösa samfund använder kamerabevakning i anslutning till sina lokaler. Tillståndskravet gäller normalt inte heller vid kamerabevakning av idrottsanläggningar eller kulturella evenemang, förutsatt att verksamheten inte bedrivs av en myndighet. Kamerabevakning inom jordbruk och skogsbruk av t.ex. stöldbegärliga maskiner omfattas normalt sett inte heller av tillståndskravet. Detsamma gäller kamerabevakning vid jakt, exempelvis vid en jaktåtel. Kamerabevakning som inte omfattas av tillståndskravet omfattas dock av lagens bestämmelser om krav på upplysning (15 §) och tystnadsplikt (22 §). Sådan kamerabevakning måste vidare bedrivas i enlighet med dataskyddsförordningen eller annan tillämplig dataskyddsreglering.

Förutsättningar för tillstånd

8 § Tillstånd till kamerabevakning ska ges om intresset av sådan bevakning väger tyngre än den enskildes intresse av att inte bli bevakad.

Vid bedömningen av intresset av kamerabevakning ska det särskilt beaktas om bevakningen behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott på en brottsutsatt plats eller på en annan plats där det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet eller på egendom,
2. förebygga, förhindra eller upptäcka störningar av allmän ordning och säkerhet eller begränsa verkningarna av sådana störningar,
3. utöva kontrollverksamhet,
4. förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor, eller
5. tillgodose andra därmed jämförliga ändamål.

Vid bedömningen av den enskildes intresse av att inte bli bevakad ska det särskilt beaktas

1. hur bevakningen ska utföras,
2. om teknik som främjar skyddet av den enskildes personliga integritet ska användas, och
3. vilket område som ska bevakas.

I paragrafen regleras förutsättningarna för att tillstånd till kamerabevakning ska ges. Paragrafen motsvarar delvis 9 § kameraövervakningslagen. Övervägandena finns i avsnitt 6.3.

Av *första stycket* framgår att tillstånd till kamerabevakning ska ges om intresset av sådan bevakning väger tyngre än den enskildes intresse av att inte bli bevakad. För att bevakningsintresset ska kunna väga tyngre än den enskildes intresse av att inte bli bevakad är en första förutsättning att det finns en rättslig grund för kamerabevakningen i den tillämpliga personuppgiftsregleringen, i första hand dataskyddsförordningen eller brottsdatalagen. Liksom enligt motsvarande bestämmelse i kameraövervakningslagen och nuvarande praxis ska sedan en helhetsbedömning av omständigheterna i det enskilda fallet göras. Det räcker att intresset av kamerabevakning väger över det motstående intresset för att tillstånd ska ges.

Enligt *andra stycket* ska vid bedömningen av intresset av kamerabevakning särskilt beaktas om kamerabevakningen behövs för vissa angivna ändamål. Att särskild hänsyn ska tas till dessa ändamål innebär att intresset av kamerabevakning i sådana fall väger tungt vid den bedömning som ska göras enligt första stycket. Tillstånd till sådan kamerabevakning kan därför ges även vid större integritetsintrång. Kamerabevakning bör många gånger betraktas som ett naturligt hjälpmedel och ett komplement till andra åtgärder. Kravet på att kamerabevakningen ska behövas för ett visst ändamål innebär därför inte att andra åtgärder nödvändigtvis måste prövas först.

Enligt *andra stycket 1* ska det särskilt beaktas om kamerabevakning behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott på en brottsutsatt plats eller på en annan plats där det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet eller på egendom.

Det ska således för det första beaktas om bevakningen behövs för brottsbekämpande ändamål på en brottsutsatt plats. Det finns inte någon begränsning av vilka brott som avses. Bestämmelsen tar alltså sikte på brott i allmänhet, t.ex. våldsbrott, stöldbrott, narkotikabrott eller skadegörelse.

Med en brottsutsatt plats menas en plats där det finns problem med brottslighet. Med detta avses inte varje plats där det någon gång har inträffat enstaka brott. Däremot krävs inte att brottsligheten är ovanligt hög på platsen i förhållande till andra jämförbara platser för att platsen ska betraktas som brottsutsatt. Sökanden behöver alltså inte presentera jämförande statistik över brottsligheten på olika platser för att tillstånd ska kunna ges. Det behöver inte heller visas att det finns påtagliga problem med brottslighet just inom ett tänkt upptagningsområde för kamerabevakningen. Det räcker således att visa att det finns problem med brottslighet på ett torg, en gågata eller inom ett stationsområde, även om ansökan om tillstånd till kamerabevakning bara avser en mindre del av torget, gågatan eller stationsområdet. På motsvarande sätt kan kamerabevakning av en viss plats inom ett bostadsområde motiveras av att bostadsområdet i stort är brottsutsatt. Vissa typer av platser kan dessutom på grundval av platsens karaktär förutsättas vara brottsutsatta utan att detta behöver bevisas i det enskilda fallet. Det kan exempelvis handla om vissa knutpunkter för allmänna kommunikationer eller om gränsövergångar där det behövs insatser mot smugglingsbrott.

För det andra ska särskild hänsyn enligt andra stycket 1 tas till om kamerabevakningen behövs på en annan plats där det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet eller på egendom. Med detta avses i första hand platser som inte kan anses vara brottsutsatta i den mening som avses i första ledet i punkten men där det ändå finns en särskild risk för vissa typer av brott jämfört med andra platser i samhället. Det kan t.ex. röra sig om platser där olika typer av angrepp i och för sig har inträffat men också om platser där det av andra skäl kan konstateras en förhöjd hotbild mot människor som vistas på platsen eller mot egendom som finns där. Som exempel kan nämnas asylboenden eller vissa myndigheters entréer, lokaler och fordon.

Med angrepp på någons liv, hälsa eller trygghet avses bl.a. misshandelsbrott, olaga tvång, olaga hot, våld eller hot mot tjänsteman, ofredande och sexualbrott, våldsamt upplopp och terroristbrott. Med angrepp på egendom avses brott som innebär förstörelse av egendom, t.ex. skadegörelse och mordbrand, men däremot inte andra brott som avser egendom, t.ex. fickstölder.

Tillstånd till kamerabevakning som aves i andra stycket 1 bör därmed många gånger kunna ges för att motverka brott och öka tryggheten i särskilt utsatta bostadsområden, på förläggningar för asylsökande, på inrättningar för hälso- och sjukvård samt på bussar, tåg, spårvagnar och andra färdmedel avsedda för allmän personbefordran, liksom vid stationer och hållplatser. Detsamma gäller för kamerabevakning som ska motverka terrorangrepp, angrepp på polismän, brandkårs- och ambulanspersonal och liknande yrkeskategorier, eller övergrepp – exempelvis sexuella ofredanden – i samband med stora folksamlingar.

För att kamerabevakning i brottsbekämpande syften ska vara verkningsfullt och materialet kunna användas i utredningar och vid lagföring krävs regelmässigt en rätt att spela in bildmaterial. Inspelning av ljud bör dock i normalfallet betraktas som särskilt integritetskänsligt och bli föremål för en särskilt noggrann prövning i det enskilda fallet. Om integritetsintrånget kan minimeras genom att tekniken arrangeras så att den endast reagerar på specifika ljud som skottlossning eller liknande, bör

det dock normalt kunna godtas att ljudupptagning sker, om behovet finns. Ljudupptagning bör exempelvis också kunna godtas i samband med utlösandet av ett överfallslarm, t.ex. i myndigheters lokaler.

Av *andra stycket 2* följer att det också ska beaktas särskilt om kamerabevakning behövs för att förebygga, förhindra eller upptäcka störningar av allmän ordning och säkerhet eller begränsa verkningarna av sådana störningar. Intresset av allmän ordning och säkerhet kan åberopas av både myndigheter och andra som har ett ansvar för ordning och säkerhet som följer av författning, t.ex. ordningslagen (1993:1617). Exempel på sådana aktörer är Polismyndigheten och kommunala myndigheter samt subjekt som bedriver kollektivtrafik. Begreppet allmän ordning och säkerhet bör tolkas på samma sätt som i andra författningar där det förekommer, t.ex. polislagen (1984:387), skyddslagen (2010:305) och ordningslagen. En kommun bör med stöd av denna punkt kunna beviljas tillstånd till kamerabevakning på platser där det regelmässigt förekommer brottslighet och andra ordningsstörningar.

Enligt *andra stycket 3* ska det särskilt beaktas om kamerabevakning behövs för att utöva kontrollverksamhet. Som exempel kan nämnas gränskontroll och tullkontroll samt kontroll av vattenskyddsområden, dammsäkerhet och miljöfarliga verksamheter.

Vidare ska det enligt *andra stycket 4* särskilt beaktas om kamerabevakning behövs för att förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor. Punkten omfattar inte bara olyckor som kan drabba människors liv och hälsa utan även olyckor som kan drabba egendom och miljön.

Slutligen följer av *andra stycket 5* att det särskilt ska beaktas om kamerabevakning behövs för att tillgodose andra därmed jämförliga ändamål, dvs. ändamål som är jämförbara med ändamålen i punkterna 1–4. Exempel på sådan kamerabevakning är kamerabevakning för utförande av en uppgift som avser Sveriges säkerhet och som inte omfattas av de tidigare punkterna samt kamerabevakning i samband med forskning som avser hur olyckor kan undvikas, t.ex. i trafiken. Ytterligare ett exempel är myndigheters kamerabevakning i samband med övningar och testverksamhet som anknyter till de ändamål som anges särskilt i punkterna 1–4.

Även andra ändamål än de som anges i punkterna 1–5 kan vara berättigade och innebära att intresset av kamerabevakning väger över den enskildes intresse av att inte bli bevakad. Ett sådant exempel är kamerabevakning för inventering av djur eller annan viltvård. Det är alltså möjligt att få tillstånd till kamerabevakning även i sådana fall men det kan behövas mer ingående överväganden av behovet av kamerabevakning i förhållande till integritetsriskerna och av hur dessa risker kan minskas.

Enligt *tredje stycket* ska det vid bedömningen av den enskildes intresse av att inte bli bevakad särskilt beaktas hur bevakningen ska utföras, om teknik som främjar skyddet av den enskildes personliga integritet ska användas och vilket område som ska bevakas.

Med hur bevakningen ska utföras avses bl.a. vid vilka tidpunkter bevakningen ska ske, om material ska spelas in och hur det i så fall kan komma att användas.

Som exempel på integritetsfrämjande teknik kan nämnas teknik som innebär att personer maskeras eller att upptaget bild- och ljudmaterial

krypteras. Ett annat exempel är kameror som aktiveras först efter olika typer av larm, såsom inbrottslarm, överfallslarm och larm som reagerar på onormala kroppsrörelser eller aktiveras av ljud som t.ex. skottlossning, glaskross eller människoskrik. Användning av integritetsfrämjande teknik kan många gånger ha stor betydelse för hur tungt intresset av att inte bli kamerabevakad väger och medföra att intresset av kamerabevakningen väger över.

När det gäller det område som ska bevakas är det av betydelse om det är ett område där många människor normalt rör sig. Det gäller oavsett om bevakningen ska ske från ett fast eller ett rörligt objekt. Områdets karaktär är också av betydelse. Exempelvis är enskildas intresse av att inte bli bevakade särskilt starkt i anslutning till deras hem, i omklädningsrum och på liknande platser.

Undantag från tillståndskravet

9 § Tillstånd till kamerabevakning krävs inte vid

1. bevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning,
2. bevakning som sker för att skydda en byggnad, en annan anläggning eller ett område som enligt 4 § 4, 5 § 1–5 eller 6 § första stycket skyddslagen (2010:305) har förklarats vara skyddsobjekt, om bevakningen endast omfattar skyddsobjektet eller ett område i dess omedelbara närhet,
3. bevakning som Försvarsmakten bedriver från ett fordon, fartyg eller luftfartyg som ett led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan bevakning,
4. bevakning som Trafikverket bedriver
   a) av vägtrafik,
   b) av sjötrafik vid en rörlig bro,
   c) vid en betalstation som avses i bilagorna till lagen (2004:629) om trängselskatt och som sker för att samla in uppgifter som behövs för att beslut om trängselskatt ska kunna fattas och för att kontrollera att sådan skatt betalas, eller
   d) vid en betalstation på allmän väg som används vid uttag av infrastrukturavgifter enligt lagen (2014:52) om infrastrukturavgifter på väg och som sker för att samla in uppgifter som behövs för att beslut om infrastrukturavgift ska kunna fattas och för att kontrollera att sådan avgift betalas,
5. bevakning i en vägtunnel med övervakningssystem som avses i lagen (2006:418) om säkerhet i vägtunnlar och som bedrivs av någon annan tunnelhållare än Trafikverket,
6. bevakning i en tunnelbanevagn eller av en tunnelbanestation, om bevakningen har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott eller förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor,
7. bevakning i en lokal där det bedrivs postverksamhet eller av området omedelbart utanför in- och utgångar till en sådan lokal, om bevakningen har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott,
8. bevakning i ett parkeringshus, om bevakningen har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott, och
9. bevakning som sker för säkerheten i trafiken eller arbetsmiljön från ett fordon, en maskin eller liknande för att förbättra sikten för föraren eller användaren.

Paragrafen, som i huvudsak motsvarar 10 § kameraövervakningslagen, reglerar undantag från kravet på tillstånd till kamerabevakning i 7 §. Övervägandena finns i avsnitt 6.5.

Undantaget i *punkten 1* avser bevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning och motsvarar 10 § första stycket 4 kameraövervakningslagen.

Enligt *punkten 2* krävs inget tillstånd vid bevakning som sker för att skydda en byggnad, en annan anläggning eller ett område som enligt 4 § 4, 5 § 1–5 eller 6 § första stycket skyddslagen har förklarats vara skyddsobjekt, om bevakningen endast omfattar skyddsobjektet eller ett område i dess omedelbara närhet. Undantaget motsvarar i huvudsak 10 § första stycket 5 kameraövervakningslagen. Till skillnad från tidigare omfattas dock samtliga skyddsobjekt enligt 4 § 4 skyddslagen, t.ex. byggnader, andra anläggningar och områden som används eller är avsedda för ledning av räddningstjänsten eller totalförsvarets civila delar. Undantaget omfattar också sådana skyddsobjekt som avses i 5 § 5 skyddslagen, dvs. områden där ett Natohögkvarter eller en främmande stats militära styrka bedriver militär verksamhet inom ramen för samförståndsavtalet den 4 september 2014 mellan Sverige och Nato om värdlandsstöd.

Undantaget i *punkten 3* avser bevakning som Försvarsmakten bedriver från ett fordon, fartyg eller luftfartyg som ett led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan bevakning. Undantaget motsvarar 10 § första stycket 6 kameraövervakningslagen.

Undantaget i *punkten 4 a* avser bevakning som Trafikverket bedriver av vägtrafik och motsvarar 10 § första stycket 2 a kameraövervakningslagen.

Enligt *punkten 4 b*, som saknar motsvarighet i kameraövervakningslagen, krävs inget tillstånd vid bevakning som Trafikverket bedriver av sjötrafik vid en rörlig bro.

Undantaget i *punkten 4 c* avser bevakning som Trafikverket bedriver vid en betalstation som avses i bilagorna till lagen om trängselskatt och som sker för att samla in uppgifter som behövs för att beslut om trängselskatt ska kunna fattas och för att kontrollera att sådan skatt betalas. Undantaget motsvarar 10 § första stycket 2 b kameraövervakningslagen.

Undantaget i *punkten 4 d* avser bevakning som Trafikverket bedriver vid en betalstation på allmän väg som används vid uttag av infrastrukturavgifter enligt lagen om infrastrukturavgifter på väg och som sker för att samla in uppgifter som behövs för att beslut om infrastrukturavgift ska kunna fattas och för att kontrollera att sådan avgift betalas. Undantaget motsvarar 10 § första stycket 2 c kameraövervakningslagen.

Undantaget i *punkten 5* avser bevakning i en vägtunnel med övervakningssystem som avses i lagen om säkerhet i vägtunnlar och som bedrivs av någon annan tunnelhållare än Trafikverket. Undantaget motsvarar 10 § första stycket 3 kameraövervakningslagen.

Undantagen i punkterna 6–8 är nya men motsvarar i huvudsak sådan kameraövervakning som tidigare varit tillåten efter anmälan enligt regleringen i kameraövervakningslagen.

Enligt *punkten 6* krävs inget tillstånd vid bevakning i en tunnelbanevagn eller av en tunnelbanestation, om bevakningen har till syfte att förebygga,

förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott eller förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor. Undantaget för tunnelbanestationer omfattar även områden innanför stationens spärrlinje som är avsedda för annan spårbunden trafik, exempelvis pendeltåg.

Enligt *punkten 7* krävs inget tillstånd vid bevakning i en lokal där det bedrivs postverksamhet eller av området omedelbart utanför in- och utgångar till en sådan lokal, om bevakningen har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott. Undantaget omfattar alla lokaler där det bedrivs postverksamhet. Begreppet postverksamhet definieras i 1 kap. 2 § postlagen (2010:1045).

Enligt *punkten* 8 krävs inte tillstånd vid bevakning i ett parkeringshus, om bevakningen har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott.

Undantaget i *punkten 9* avser bevakning som sker för säkerheten i trafiken eller arbetsmiljön från ett fordon, en maskin eller liknande för att förbättra sikten för föraren eller användaren. Undantaget motsvarar 10 § första stycket 1 kameraövervakningslagen.

Undantagen från tillståndskravet gäller all kamerabevakning enligt 3 § 1–3 och omfattar därmed också avlyssning och upptagning av ljud.

Tillfälliga undantag från tillståndskravet

10 § Kamerabevakning får ske utan att en ansökan om tillstånd har gjorts

1. under högst tre månader, vid bevakning som bedrivs av Polismyndigheten eller Säkerhetspolisen, om det av särskild anledning finns risk för allvarlig brottslighet och syftet med bevakningen är att förebygga, förhindra eller upptäcka sådan brottslig verksamhet eller utreda eller lagföra sådana brott,
2. under högst en månad, vid bevakning som bedrivs av Polismyndigheten eller den som är räddningsledare enligt lagen (2003:778) om skydd mot olyckor, om bevakningen är av vikt för att avvärja en överhängande fara för olycka, begränsa verkningarna av en inträffad olycka eller minska risken för nya olyckor, eller
3. under högst en månad, vid bevakning som bedrivs av den som är räddningsledare enligt lagen om skydd mot olyckor, om bevakningen är av vikt för att efterforska en försvunnen person.

Om en ansökan om tillstånd görs inom den tid som anges i första stycket, får bevakningen bedrivas utan tillstånd till dess att ansökan har prövats.

Paragrafen reglerar tillfälliga undantag från kravet på tillstånd till kamerabevakning i 8 §. Paragrafen motsvarar huvudsakligen 11 § kameraövervakningslagen. Övervägandena finns i avsnitt 6.6.

Enligt *första stycket 1* får Polismyndigheten eller Säkerhetspolisen under högst tre månader bedriva kamerabevakning utan att en ansökan om tillstånd har gjorts, om det av särskild anledning finns risk för allvarlig brottslighet och syftet med bevakningen är att förebygga, förhindra eller upptäcka sådan brottslig verksamhet eller utreda eller lagföra sådana brott. Det krävs inte misstanke om ett konkret allvarligt brott utan det räcker att det av särskild anledning finns risk för allvarlig brottslighet. Med allvarlig brottslighet avses bl.a. angrepp på någons liv, och allvarliga angrepp på hälsa eller trygghet, t.ex. grov våldsbrottslighet eller systematiska fall av sexuella övergrepp. Andra exempel är omfattande förstörelse av egendom eller omfattande narkotikahandel.

Enligt *första stycket 2* får Polismyndigheten eller den som är räddningsledare enligt lagen om skydd mot olyckor (LSO) bedriva kamerabevakning utan att en ansökan om tillstånd har gjorts under högst en månad i samband med olyckor. Undantaget omfattar även åtgärder på grund av överhängande fara för olycka samt efterföljande åtgärder enligt 3 kap. 9 § och 4 kap. 7 § LSO. Innebörden av uttrycket överhängande fara för olycka är densamma som i lagen om skydd mot olyckor.

Enligt *första stycket 3* får den som är räddningsledare enligt lagen om skydd mot olyckor även bedriva kamerabevakning utan att en ansökan om tillstånd har gjorts under högst en månad om bevakningen är av vikt för att efterforska en försvunnen person. Undantaget är tillämpligt även när någon annan biträder räddningsledaren.

Av *andra stycket* följer att om en ansökan om tillstånd görs inom den tid som undantaget gäller, får kamerabevakningen fortsätta att bedrivas utan tillstånd fram till dess att ansökan har prövats av tillsynsmyndigheten.

Ansökan om tillstånd

11 § En ansökan om tillstånd till kamerabevakning ska göras skriftligen hos tillsynsmyndigheten.

Ansökan ska innehålla

1. uppgift om den som ska bedriva bevakningen och i förekommande fall den som ska ha hand om bevakningen för tillståndshavarens räkning,
2. uppgift om bevakningens ändamål,
3. en beskrivning av bevakningen, särskilt den utrustning som ska användas, var utrustningen ska placeras, det område eller typ av område som ska bevakas och de tider då bevakning ska ske,
4. en bedömning av behovet av bevakningen och bevakningens proportionalitet i förhållande till ändamålet,
5. en bedömning av riskerna för intrång i den personliga integriteten och en beskrivning av de åtgärder som planeras för att hantera riskerna, och
6. uppgift om de omständigheter i övrigt som är av betydelse för prövningen av ärendet.

Om sökanden inte är en myndighet, ska ansökan innehålla uppgift om den lag eller annan författning, kollektivavtal eller beslut som utgör den rättsliga grunden för kamerabevakningen.

Om bevakningen avser en arbetsplats, ska ett yttrande från ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på arbetsplatsen lämnas in tillsammans med ansökan.

I paragrafen, som delvis motsvarar 17 § kameraövervakningslagen, finns bestämmelser om innehållet i en ansökan om tillstånd. Övervägandena finns i avsnitt 6.4.

Av *första stycket* följer att en ansökan om tillstånd ska vara skriftlig och göras hos tillsynsmyndigheten.

I *andra stycket* anges att ansökan ska innehålla 1) uppgift om den som ska bedriva bevakningen och i förekommande fall den som ska ha hand om bevakningen för tillståndshavarens räkning, 2) uppgift om bevakningens ändamål, 3) en beskrivning av bevakningen, särskilt den utrustning som ska användas, var utrustningen ska placeras, det område eller typ av område som ska bevakas och de tider då bevakning ska ske, 4) en bedömning av behovet av bevakningen och bevakningens proportionalitet i förhållande till ändamålet, 5) en bedömning av riskerna

för intrång i den personliga integriteten och en beskrivning av de åtgärder som planeras för att hantera riskerna, och 6) uppgift om de omständigheter i övrigt som är av betydelse för prövningen av ärendet. Punkterna 4 och 5 är nya i förhållande till kameraövervakningslagen. Den som bedriver kamerabevakning av flera liknande platser för samma ändamål bör ofta kunna ta fram sådana behovs- och riskbedömningar som kan användas vid flera bevakningssituationer.

Enligt *tredje stycket* ska ansökan, om sökanden inte är en myndighet, innehålla uppgift om den lag eller annan författning, kollektivavtal eller beslut som utgör den rättsliga grunden för kamerabevakningen.

Enligt *fjärde stycket* ska sökanden, om kamerabevakningen avser en arbetsplats, tillsammans med ansökan lämna in ett yttrande från ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på arbetsplatsen. Bestämmelsen gäller när en arbetsgivare ansöker om kamerabevakning. Flera yttranden kan krävas, om det finns olika arbetstagargrupper på arbetsplatsen. Om det inte finns någon företrädare av det aktuella slaget bortfaller däremot kravet. I yttrandet bör anges om bevakningen godtas eller inte. Om den inte godtas, bör skälen för det framgå.

Yttrande av kommunen

12 § Innan tillsynsmyndigheten beslutar om tillstånd till kamerabevakning ska den kommun där bevakningen ska ske få tillfälle att yttra sig, om det av särskild anledning behövs ett yttrande.

I paragrafen regleras i vilka fall den kommun där kamerabevakningen ska ske ska få tillfälle att yttra sig över en ansökan om kamerabevakning. Paragrafen motsvarar delvis 18 § kameraövervakningslagen. Övervägandena finns i avsnitt 6.4.

Av paragrafen följer att tillsynsmyndigheten i ett ärende om tillstånd till kamerabevakning ska ge den kommun där bevakningen ska ske tillfälle att yttra sig, om det av särskild anledning behövs ett yttrande. Syftet med bestämmelsen är att säkerställa att lokala synpunkter beaktas i ärendet när sådana kan vara av särskild betydelse. Ett exempel på detta är om ansökan gäller omfattande och varaktig kamerabevakning av centrala stadsdelar eller bevakning av en plats där flera kommunala evenemang väntas äga rum. Det torde mycket sällan finnas anledning att inhämta yttranden från kommunen vid kamerabevakning med drönare eller från fordon.

Beslut om tillstånd

13 § I ett beslut om tillstånd till kamerabevakning ska det anges vem som ska bedriva bevakningen och i förekommande fall vem som ska ha hand om bevakningen för tillståndshavarens räkning.

Beslutet ska förenas med villkor om hur kamerabevakningen får anordnas. Villkoren ska avse

1. bevakningens ändamål,
2. den utrustning som får användas och var utrustningen får placeras,
3. det område eller typ av område som får bevakas och de tider då bevakning får ske, och

4. upplysning om bevakningen, bevarande eller annan behandling av bilder eller ljud och andra förhållanden som har betydelse för att skydda enskildas personliga integritet, om sådana villkor behövs för tillståndet.

Ett tillstånd får meddelas för en begränsad tid.

Paragrafen reglerar vad tillsynsmyndighetens beslut om tillstånd till kamerabevakning ska innehålla. Paragrafen motsvarar i huvudsak 19 § kameraövervakningslagen. Övervägandena finns i avsnitt 6.4.

Enligt *första* stycket ska det i ett beslut om tillstånd till kamerabevakning anges vem som ska bedriva bevakningen och i förekommande fall vem som ska ha hand om bevakningen för tillståndshavarens räkning.

Enligt *andra* stycket ska beslutet om tillstånd förenas med villkor om hur kamerabevakningen får anordnas. Villkoren ska avse 1) bevakningens ändamål, 2) den utrustning som får användas och var utrustningen får placeras, 3) det område eller typ av område som får bevakas och de tider då bevakning får ske, och 4) upplysning om bevakningen, bevarande eller annan behandling av bilder eller ljud och andra förhållanden som har betydelse för att skydda enskildas personliga integritet, om sådana villkor behövs för tillståndet

Som utgångspunkt bör en tillståndshavare ha ett visst utrymme att flytta eller byta ut kameror inom samma område, i vart fall så länge det inte innebär att integritetsriskerna ökar. Tillsynsmyndigheten bör därför inte föreskriva mer detaljerade villkor än vad som behövs för att exempelvis avgränsa ett visst bevakningsområde eller knyta beslutet till en viss typ av teknik. Vid kamerabevakning från rörliga objekt kan det ofta finnas skäl att meddela villkor om vilken typ av område som får bevakas. Sådana villkor kan också vid behov utformas på ett sätt som reglerar var bevakning inte får ske, t.ex. i närheten av bostadsbebyggelse eller friluftsområden.

Enligt *tredje stycket* får ett tillstånd meddelas för en begränsad tid.

Ändrade förhållanden

14 § Om förutsättningarna för ett tillstånd ändras, får tillsynsmyndigheten besluta om nya villkor eller, om förutsättningarna för tillstånd inte längre är uppfyllda, återkalla tillståndet.

Paragrafen reglerar möjligheten för tillsynsmyndigheten att besluta om nya villkor eller återkalla tillståndet. Paragrafen motsvarar delvis 20 § kameraövervakningslagen. Övervägandena finns i avsnitt 6.4.

Upplysning om kamerabevakning och enskildas rätt till information

Krav på upplysning

15 § Upplysning om kamerabevakning ska lämnas genom tydlig skyltning eller på något annat verksamt sätt.

Om ljud kan avlyssnas eller tas upp vid bevakningen, ska en särskild upplysning lämnas om detta.

Bestämmelser om rätten till information om den personuppgiftsbehandling som kamerabevakningen innebär finns i EU:s dataskyddsförordning och andra föreskrifter som anges i 6 §.

Paragrafen reglerar kravet på upplysning vid kamerabevakning. Paragrafen motsvarar delvis 25 § kameraövervakningslagen. Övervägandena finns i avsnitt 7.1.

Enligt *första stycket* ska upplysning om kamerabevakning lämnas genom tydlig skyltning eller på något annat verksamt sätt. Det vanligaste sättet att uppfylla kravet på upplysning är genom tydlig skyltning i direkt anslutning till den plats som kamerabevakas. Om kamerabevakningen ska ske från ett fordon kan en sådan skylt eller dekal i stället lämpligen placeras på fordonet så att den är väl synlig utifrån. Vid kamerabevakning från exempelvis drönare kan upplysning i vissa fall lämnas genom skyltning eller andra typer av markeringar eller avspärrningar på marken, t.ex. i utkanten av det bevakade området. I annat fall får upplysning lämnas på något annat verksamt och lämpligt sätt, t.ex. genom att information om bevakningen lämnas direkt till dem som kan komma att omfattas av den.

Om ljud kan avlyssnas eller tas upp vid bevakningen ska enligt *andra stycket* en särskild upplysning lämnas om detta.

Tredje stycket innehåller en upplysning om att det finns bestämmelser om enskildas rätt till information om den personuppgiftsbehandling som kamerabevakningen innebär i dataskyddsförordningen och de andra föreskrifter som anges i 6 §. Hänvisningen till dataskyddsförordningen avser förordningen i den vid varje tidpunkt gällande lydelsen. Utöver kravet på upplysning i kamerabevakningslagen gäller alltså bestämmelser i annan personuppgiftsreglering, exempelvis dataskyddsförordningen eller brottsdatalagen, om att den som är personuppgiftsansvarig ska lämna information till den registrerade om den personuppgiftsbehandling som kamerabevakningen innebär. Det handlar t.ex. om den personuppgiftsansvariges identitet och kontaktuppgifter, dataskyddsombudets kontaktuppgifter i tillämpliga fall, ändamålen med behandlingen och rätten att inge klagomål till tillsynsmyndigheten. Sådan ytterligare information kan visserligen lämnas på en skylt som upplyser om kamerabevakningen men den kan också göras tillgänglig för den registrerade på något annat sätt, exempelvis genom en hänvisning till en webbsida. Enligt regleringen i dataskyddsförordningen finns vissa undantag från skyldigheten att lämna information, bl.a. om den registrerade redan förfogar över informationen.

Undantag från upplysningskravet och rätten till information

16 § Upplysning om kamerabevakning och information om den personuppgiftsbehandling som kamerabevakningen innebär behöver inte lämnas vid

1. bevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning,
2. bevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller Säkerhetspolisen, om det av särskild anledning finns risk för allvarlig brottslighet och syftet med bevakningen är att förebygga, förhindra eller upptäcka sådan brottslig verksamhet eller utreda eller lagföra sådana brott,
3. bevakning som sker för att skydda en byggnad, en annan anläggning eller ett område som enligt 4 § 4, 5 § 1–5 eller 6 § första stycket skyddslagen (2010:305) har förklarats vara skyddsobjekt, om bevakningen endast omfattar skyddsobjektet eller ett område i dess omedelbara närhet,

4. bevakning som Försvarsmakten bedriver från ett fordon, fartyg eller luftfartyg som ett led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan bevakning,

5. bevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller den som är räddningsledare enligt lagen (2003:778) om skydd mot olyckor, om bevakningen är av vikt för att avvärja en överhängande fara för olycka, begränsa verkningarna av en inträffad olycka eller minska risken för nya olyckor, och

6. bevakning som bedrivs av den som är räddningsledare enligt lagen om skydd mot olyckor, om bevakningen är av vikt för att efterforska en försvunnen person.

Undantagen i första stycket gäller inte om ljud ska avlyssnas eller tas upp vid kamerabevakningen.

Paragrafen reglerar undantag från kravet på upplysning om kamerabevakning och den rätt till information om den personuppgiftsbehandling som kamerabevakningen innebär. Undantagen i första stycket 1, 3, 4 och 6 motsvarar i huvudsak 27 § första stycket kameraövervakningslagen medan undantagen i första stycket 2 och 5 är nya. Paragrafens andra stycke motsvarar 27 § fjärde stycket kameraövervakningslagen. Övervägandena finns i avsnitt 7.2.

Paragrafen innebär att upplysning om kamerabevakning enligt 15 § inte behöver lämnas i vissa särskilt utpekade fall. I sådana fall behöver inte heller information om den personuppgiftsbehandling som kamerabevakningen innebär lämnas till den registrerade. Paragrafen utgör därmed ett undantag från artiklarna 13 och 14 i dataskyddsförordningen, 4 kap. 2 § brottsdatalagen och annan tillämplig personuppgiftreglering som reglerar enskildas rätt till information. Paragrafen innebär dock inte någon begränsning av den registrerades rätt till tillgång till personuppgifter och viss annan information enligt artikel 15 i dataskyddsförordningen och enligt 4 kap. 3 § brottsdatalagen. Paragrafen innebär inte heller någon begränsning av den personuppgiftsansvariges skyldighet att göra viss allmän information tillgänglig för registrerade enligt 4 kap. 1 § brottsdatalagen.

I *första stycket 1, 3, 4* och *6* görs undantag från kravet på upplysning och rätten till information i fall som motsvarar undantagen från tillståndskravet i 9 § 1–3 och 10 § första stycket 3.

Enligt *första stycket 2* behöver upplysning om kamerabevakningen och information om den personuppgiftsbehandling som bevakningen innebär inte lämnas vid bevakning som bedrivs från ett luftfartyg av Polismyndigheten eller Säkerhetspolisen i brådskande fall, om det av särskild anledning finns risk för allvarlig brottslighet och syftet med bevakningen är att förebygga, förhindra eller upptäcka sådan brottslig verksamhet eller utreda eller lagföra sådana brott. Undantaget motsvarar det tillfälliga undantaget från tillståndskravet i 10 § första stycket 1, se författningskommentaren till den bestämmelsen, med ett tillkommande krav på att det ska vara fråga om brådskande fall och att kamerabevakningen sker från ett luftfartyg, t.ex. en drönare. Undantaget kan vara tillämpligt t.ex. vid våldssammandrabbningar på offentliga platser, vid terrorangrepp eller vid andra plötsliga händelser som av särskild anledning innebär en risk för allvarlig brottslighet. Undantaget innefattar inte en rätt att försöka dölja kamerabevakningen eller att använda den som ett led i en pågående förundersökning.

Enligt *första stycket 5* behöver upplysning om kamerabevakningen och information om den personuppgiftsbehandling som bevakningen innebär inte lämnas vid bevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller den som är räddningsledare enligt lagen om skydd mot olyckor, om bevakningen är av vikt för att avvärja en överhängande fara för olycka, eller begränsa verkningarna av en inträffad olycka eller minska risken för nya olyckor. Undantaget motsvarar det tillfälliga undantaget från tillståndskravet i 10 § första stycket 2, se författningskommentaren till den bestämmelsen, med ett tillkommande krav på att det ska vara fråga om ett brådskande fall och att kamerabevakningen sker från ett luftfartyg, t.ex. en drönare. Så kan t.ex. vara fallet i samband med bränder eller olyckor vid anläggningar som kan orsaka allvarliga skador på många människor eller på miljön.

Att undantagen i första stycket 2 och 5 bara är tillämpliga i brådskande fall innebär att upplysning om kamerabevakningen och information om den personuppgiftsbehandling som bevakningen innebär ska lämnas när det är möjligt.

Av *andra stycket* följer att undantagen från kravet på upplysning och information i första stycket inte gäller om ljud ska avlyssnas eller tas upp vid kamerabevakningen. Om det finns behov av att kunna avlyssna eller ta upp ljud i samband med kamerabevakning utan upplysning kan undantag beviljas i enskilda fall enligt 17 §.

Undantag i enskilda fall

17 § Om det finns synnerliga skäl får tillsynsmyndigheten i enskilda fall besluta om undantag från upplysningskravet och rätten till information om den personuppgiftsbehandling som kamerabevakningen innebär.

Paragrafen reglerar undantag i enskilda fall från kravet på upplysning och rätten till information om den personuppgiftsbehandling som kamerabevakningen innebär. Paragrafen motsvarar delvis 27 § tredje stycket kameraövervakningslagen. Övervägandena finns i avsnitt 7.2.

Av paragrafen framgår att tillsynsmyndigheten får besluta om undantag från upplysningskravet i kamerabevakningslagen och rätten till information om den personuppgiftsbehandling som kamerabevakningen innebär, om det finns synnerliga skäl. Undantagsmöjligheten ska tillämpas restriktivt och tillsynsmyndigheten måste vid sin prövning i det enskilda fallet avgöra om ett undantag från rätten till information är förenligt med annan tillämplig personuppgiftsreglering.

Undantag kan beslutas i fall där syftet med angelägen kamerabevakning skulle gå förlorat om upplysning skulle lämnas om bevakningen. Exempel på sådana fall är kamerabevakning av rovdjurslyor i syfte att upptäcka och beivra tjuvskytte eller plundring eller i syfte att kartlägga rovdjursbeståndet.

Undantag kan också beslutas när upplysningskravet är praktiskt omöjligt att uppfylla, t.ex. eftersom kamerabevakningen ska ske från ett luftfartyg, såsom en drönare, och avse större områden som skiftar från gång till annan. Som exempel kan nämnas kamerabevakning i räddningsverksamhet som inte omfattas av undantagen i 16 § och Polismyndighetens användning av kamerautrustade drönare i samband med exempelvis statsbesök eller andra

planerade evenemang där bevakningen framstår som angelägen men sannolikt inte kan begränsas till ett visst område.

Undantag kan vidare komma i fråga när kamerabevakning i ett brådskande fall bedrivs utan upplysning med stöd av något av de generella undantagen i 16 § första stycket 2 och 5 och behovet av att kamerabevaka kvarstår efter det inledande, akuta skedet samtidigt som upplysningskravet inte heller då kan uppfyllas.

Ett undantag från upplysningskravet och rätten till information får omfatta avlyssning eller upptagning av ljud. Sådana undantag bör dock endast komma i fråga i särpräglade undantagsfall där intresset av kamerabevakning utan upplysning är berättigat och väger tungt samtidigt som integritetsriskerna i praktiken är obefintliga. Exempel på sådana fall är användning av kamerautrustade drönare i samband med efterforskandet av försvunna personer eller Polismyndighetens användning av sensorer som kan detektera ljud av skottlossning eller liknande. Undantaget får dock inte tillämpas på ett sätt som möjliggör hemlig eller dold avlyssning av människors samtal.

Ansökan om undantag

18 § En ansökan om sådant undantag som avses i 17 § ska göras skriftligen hos tillsynsmyndigheten.

Ansökan ska innehålla uppgift om den som ska bedriva kamerabevakningen och i förekommande fall den som ska ha hand om bevakningen för hans eller hennes räkning samt skälen för ansökan.

Om bevakningen avser en arbetsplats, ska ett yttrande från ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på arbetsplatsen lämnas in tillsammans med ansökan.

I paragrafen finns bestämmelser om innehållet i en ansökan om undantag enligt 17 §. Paragrafen motsvarar delvis 27 § andra stycket kameraövervakningslagen. Övervägandena finns i avsnitt 7.2.

Av *första stycket* följer att en ansökan om undantag ska vara skriftlig och göras hos tillsynsmyndigheten.

Enligt *andra stycket* ska ansökan innehålla uppgift om den som ska bedriva kamerabevakningen och i förekommande fall den som ska ha hand om bevakningen för hans eller hennes räkning samt skälen för ansökan. Att skälen för ansökan ska anges innebär att sökanden måste klargöra anledningen till varför det finns synnerliga skäl för undantag i det aktuella fallet. Sökanden bör i regel ange syftet med kamerabevakningen och lämna en beskrivning av bevakningen, t.ex. genom att uppge vilken utrustning som ska användas, var utrustningen ska placeras, vilket område eller typ av område som ska bevakas och vilka tider som bevakningen ska ske.

Om kamerabevakningen avser en arbetsplats, ska enligt *tredje stycket* sökanden tillsammans med ansökan lämna in ett yttrande från ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på arbetsplatsen. Bestämmelsen gäller när en arbetsgivare ansöker om kamerabevakning. I yttrandet bör anges om ett undantag från upplysningskravet godtas eller inte. Om det inte godtas, bör skälen för det framgå. Flera yttranden kan krävas, om det finns olika arbetstagargrupper på arbetsplatsen.

Yttrande av kommunen

19 § Innan tillsynsmyndigheten beslutar om sådant undantag som avses i 17 §, ska den kommun där kamerabevakningen ska ske få tillfälle att yttra sig, om bevakningen avser en plats dit allmänheten har tillträde och det av särskild anledning behövs ett yttrande.

Paragrafen reglerar i vilka fall den kommun där kamerabevakningen ska ske ska få tillfälle att yttra sig över en ansökan om undantag från upplysningskravet. Paragrafen motsvarar delvis 27 § tredje stycket kameraövervakningslagen. Övervägandena finns i avsnitt 7.2.

Av paragrafen följer att tillsynsmyndigheten i ett ärende om undantag från upplysningskravet ska ge den kommun där bevakningen ska ske tillfälle att yttra sig, om bevakningen avser en plats dit allmänheten har tillträde och det av särskild anledning behövs ett yttrande, jfr författningskommentaren till 12 §.

Beslut om undantag

20 § I ett beslut om undantag enligt 17 § ska det anges vem som ska bedriva kamerabevakningen och i förekommande fall vem som ska ha hand om bevakningen för hans eller hennes räkning. Beslutet ska förenas med de villkor som behövs och får meddelas för en begränsad tid.

Om förutsättningarna för ett beslut om undantag ändras, får tillsynsmyndigheten besluta om nya villkor eller, om förutsättningarna för ett sådant beslut inte längre är uppfyllda, återkalla beslutet.

Paragrafen reglerar innehållet i tillsynsmyndighetens beslut om undantag enligt 17 § och myndighetens möjlighet att ändra eller återkalla ett sådant beslut. Paragrafen motsvarar delvis 27 § tredje stycket kameraövervakningslagen. Övervägandena finns i avsnitt 7.2.

Tillsynsmyndigheten ska enligt *första stycket* i ett beslut om undantag ange vem som ska bedriva kamerabevakningen och i förekommande fall vem som ska ha hand om bevakningen för dennes räkning. Vidare ska ett sådant beslut förenas med de villkor som behövs. Det kan ofta bli fråga om samma typer av villkor som beslut om tillstånd till kamerabevakning enligt 13 § andra stycket ska förenas med, se författningskommentaren till den paragrafen. Beslutet kan precis som ett tillståndsbeslut begränsas till att gälla för en viss tid.

Enligt *andra stycket* får tillsynsmyndigheten besluta om nya villkor, om förutsättningarna för beslutet ändras. Om förutsättningarna inte längre är uppfyllda får myndigheten återkalla beslutet.

Förhandlingsskyldighet för arbetsgivare

21 § I fråga om arbetsgivares beslut om kamerabevakning av en arbetsplats, finns bestämmelser om förhandlingsskyldighet i 11–14 §§ lagen (1976:580) om medbestämmande i arbetslivet.

Paragrafen upplyser om att det i fråga om arbetsgivares kamerabevakning av en arbetsplats, finns bestämmelser om förhandlingsskyldighet i lagen om medbestämmande i arbetslivet. Paragrafen saknar motsvarighet i kameraövervakningslagen. Övervägandena finns i avsnitt 8.

Bestämmelsen tar sikte på de fall där en arbetsgivare bedriver kamerabevakning. Det saknas betydelse om det rör sig om kamerabevakning av utrymmen på arbetsplatsen dit allmänheten har tillträde eller inte.

Förhandlingsskyldigheten i 11 § MBL får normalt anses gälla inför arbetsgivares beslut om kamerabevakning som innebär att anställda varaktigt eller regelbundet bevakas. Dessutom har arbetstagarorganisationerna en möjlighet att påkalla förhandling på eget initiativ enligt 12 § MBL. Att ett krav på tillstånd i vissa fall gäller för kamerabevakningen ersätter inte ett sådant förfarande som regleras i lagen om medbestämmande i arbetslivet. Mot vem och hur förhandlingsskyldigheten ska fullgöras framgår av 11–14 §§ MBL. Frågor om skadestånd, preskription och sanktioner m.m. vid överträdelser av aktuella bestämmelser styrs också av den arbetsrättsliga regleringen och inte av dataskyddsförordningen eller kamerabevakningslagen.

Tystnadsplikt och utlämnande av uppgifter

22 § Den som tar befattning med en uppgift som har inhämtats genom kamerabevakning får inte obehörigen röja eller utnyttja det som han eller hon på detta sätt har fått veta om någon enskilds personliga förhållanden.

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

Paragrafen reglerar tystnadsplikt för den som tar befattning med uppgifter som inhämtas genom kamerabevakning. Paragrafen motsvarar 37 § kameraövervakningslagen. Övervägandena finns i avsnitt 10.

Av *första stycket* framgår att den som tar befattning med en uppgift som har inhämtats genom kamerabevakning inte obehörigen får röja eller utnyttja det som han eller hon på detta sätt har fått veta om någon enskilds personliga förhållanden. Bestämmelsen gäller både uppgifter som inhämtas i realtid och uppgifter som har inhämtats ur inspelat bild- och ljudmaterial. Det är inte bara spridning av själva materialet som omfattas utan även röjande eller utnyttjande av uppgifter ur materialet.

Obehörighetsrekvisitet är avsett att tolkas på så sätt att ett uppgiftslämnande av en enskild aktör som motsvarar ett uppgiftslämnande som är tillåtet enligt offentlighets- och sekretesslagen inte är att betrakta som obehörigt. Bestämmelsen i 32 kap. 3 § OSL som särskilt tar sikte på uppgifter som har inhämtats genom kamerabevakning har ett omvänt skaderekvisit. Det innebär att sekretess gäller, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider men. Därmed är det inte fråga om ett obehörigt utlämnande enligt paragrafen, om det står klart att den uppgift det gäller kan lämnas ut utan att den enskilde eller någon närstående till den enskilde lider men. Frågan om en uppgift omfattas av tystnadsplikt beror alltså på hur känslig uppgiften är. Om den som uppgiften avser samtycker till ett utlämnande är det inte fråga om ett obehörigt utlämnande.

Bestämmelsen omfattar exempelvis tillgängliggörande av bilder via en webbkamera under förutsättning att användningen faller inom kamerabevakningslagens tillämpningsområde. Huruvida ett sådant tillgängliggörande innebär ett obehörigt utlämnande får avgöras i det enskilda

fallet. Bestämmelsen omfattar formellt även den situationen att bilder från kamerabevakning visas för förbipasserande via en bildskärm i anslutning till kameran. Ett sådant röjande bör emellertid inte anses vara obehörigt eftersom bilderna endast visar det som de förbipasserande kan se även utan tillgång till bildskärmen.

Ett utlämnande som är tillåtet enligt den sekretessbrytande bestämmelsen i 32 kap. 3 a § OSL är tillåtet också enligt förevarande paragraf. Enskilda som bedriver kamerabevakning får alltså lämna ut inspelat material till en åklagarmyndighet, Polismyndigheten, Tullverket, Kustbevakningen eller Skatteverket, om uppgiften behövs för att utreda ett begånget brott för vilket fängelse är föreskrivet eller för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket fängelse är föreskrivet. Ett utlämnande får vidare ske till en kommun eller en myndighet som ansvarar för räddningstjänst enligt lagen om skydd mot olyckor, om uppgiften behövs för att förebygga en hotande olycka eller för att begränsa verkningarna av en redan inträffad olycka.

Den som bryter mot paragrafen kan dömas för brott mot tystnadsplikt enligt 20 kap. 3 § brottsbalken.

Andra stycket innehåller en erinran om att offentlighets- och sekretesslagen i stället tillämpas i det allmännas verksamhet.

Tillsyn, sanktionsavgifter och skadestånd

Tillsynsmyndighet

23 § Den myndighet som regeringen bestämmer utövar tillsyn över kamerabevakning enligt denna lag.

I paragrafen, som delvis motsvarar 38–40 §§ kameraövervakningslagen, anges att den myndighet som regeringen bestämmer utövar tillsyn över kamerabevakning enligt lagen. Övervägandena finns i avsnitt 11.1.

Tillsynen tar sikte på att lagens bestämmelser samt beslut som meddelats med stöd av lagen följs. Som framgår av 11 och 17 §§ är det tillsynsmyndigheten som prövar ansökningar om tillstånd till kamerabevakning och om undantag från upplysningskravet och rätten till information.

Befogenheter

24 § Bestämmelser om tillsynsmyndighetens befogenheter i EU:s dataskyddsförordning och de föreskrifter som anges i 6 § ska gälla även vid tillsynen över att denna lag följs.

Paragrafen handlar om tillsynsmyndighetens befogenheter och motsvarar delvis 41–43 §§ kameraövervakningslagen. Övervägandena finns i avsnitt 11.2.

Av paragrafen framgår att de befogenheter som tillsynsmyndigheten har enligt dataskyddsförordningen och föreskrifter som avses i 6 §, t.ex. dataskyddslagen och brottsdatalagen, ska gälla även vid tillsynen över att kamerabevakningslagen följs. Detta innebär att bestämmelserna om tillsynsmyndighetens befogenheter i artikel 58 i dataskyddsförordningen, liksom andra tillämpliga bestämmelser om befogenheter i föreskrifter som

kompletterar förordningen, ska tillämpas vid sådan kamerabevakning som omfattas av förordningens tillämpningsområde. Hänvisningen till dataskyddsförordningen avser förordningen i den vid varje tidpunkt gällande lydelsen. Vid kamerabevakning som omfattas av brottsdatalagens tillämpningsområde ska i stället bestämmelserna i 5 kap. 5–7 §§ den lagen eller andra tillämpliga föreskrifter som genomför dataskyddsdirektivet tillämpas. Regleringen i 1 kap. 2 § dataskyddslagen innebär att bestämmelserna i dataskyddsförordningen gäller även vid behandling av personuppgifter som varken omfattas av dataskyddsförordningens eller brottsdatalagens tillämpningsområde, t.ex. inom verksamhet som rör den nationella säkerheten. Av dataskyddslagen följer också att om det finns avvikande reglering om tillsyn för sådan verksamhet, t.ex. i en registerförfattning, ska de bestämmelserna tillämpas i stället.

Bestämmelsen innebär också att tillsynsmyndigheten kan använda befogenheterna i samband med handläggning av ärenden enligt lagen eller när den som bedriver bevakningen underlåter att bistå myndigheten i ett sådant ärende. Med tillsynsmyndigheten avses den myndighet som utövar tillsyn enligt kamerabevakningslagen med stöd av 23 §.

Sanktionsavgifter

25 § Tillsynsmyndigheten får ta ut en sanktionsavgift av den som bedriver kamerabevakning och

1. bryter mot tillståndskravet i 7 §,
2. inte följer villkor i ett beslut om tillstånd som har meddelats med stöd av 13 eller 14 §§,
3. bryter mot upplysningskravet i 15 §, eller
4. inte följer villkor i ett beslut om undantag som har meddelats med stöd av 20 §.

Paragrafen, som saknar motsvarighet i kameraövervakningslagen, anger i vilka fall tillsynsmyndigheten får ta ut en sanktionsavgift av den som bedriver kamerabevakning. Övervägandena finns i avsnitt 11.2.

Enligt *punkten 1* får tillsynsmyndigheten ta ut en sanktionsavgift av den som bedriver kamerabevakning och bryter mot tillståndskravet i 7 §, dvs. saknar tillstånd till kamerabevakning trots att ett sådant krävs enligt lagen.

En sanktionsavgift får enligt *punkten 2* också tas ut av den som har beviljats tillstånd till kamerabevakning men inte följer villkoren i beslutet om hur kamerabevakningen får anordnas.

Tillsynsmyndigheten får vidare enligt *punkten 3* ta ut en sanktionsavgift av den som bedriver kamerabevakning och bryter mot kraven i 15 § om hur upplysning om kamerabevakning ska lämnas.

En sanktionsavgift får enligt *punkten 4* också tas ut av den som har beviljats undantag från upplysningskravet och rätten till information men inte följer villkoren i beslutet om undantag.

26 § Vid beslut om sanktionsavgift ska artikel 83.1, 83.2 och 83.3 i EU:s dataskyddsförordning, i den ursprungliga lydelsen, och 6 kap. 4–7 §§ lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning tillämpas. Vid kamerabevakning som omfattas av brottsdatalagen (2018:000) ska i stället 6 kap. 3 § tredje stycket och 6 kap. 4–9 §§ den lagen tillämpas.

Paragrafen reglerar vilka bestämmelser som ska tillämpas vid beslut om sanktionsavgift. Paragrafen saknar motsvarighet i kameraövervakningslagen. Övervägandena finns i avsnitt 11.2.

Av paragrafen följer att artikel 83.1, 83.2 och 83.3 i dataskyddsförordningen samt 6 kap. 4–7 §§ dataskyddslagen i första hand ska tillämpas vid beslut om sanktionsavgift. Dataskyddsförordningens och dataskyddslagens bestämmelser ska därmed tillämpas både vid sådan kamerabevakning som omfattas av förordningens tillämpningsområde och vid sådan kamerabevakning som faller utanför EU-rättens tillämpningsområde. Hänvisningen till dataskyddsförordningen är statisk, dvs. avser den ursprungliga lydelsen av förordningen. Eftersom hänvisning även sker till 6 kap. 7 § dataskyddslagen gäller också de ytterligare föreskrifter om sanktionsavgifter som meddelas i anslutning till dataskyddslagen. För kamerabevakning som omfattas av brottsdatalagens tillämpningsområde ska 6 kap. 3 § tredje stycket och 4–9 §§ den lagen tillämpas i stället.

27 § Vid sådana överträdelser som avses i 25 § 1 och 2 ska avgiftens storlek bestämmas med tillämpning av artikel 83.4 i EU:s dataskyddsförordning, i den ursprungliga lydelsen, eller, i fråga om myndigheter, med tillämpning av den lägre avgiftsnivån i 6 kap. 2 § andra stycket lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning. Vid kamerabevakning som omfattas av brottsdatalagen ska avgiftens storlek i stället bestämmas med tillämpning av 6 kap. 3 § första stycket den lagen.

Vid sådana överträdelser som avses i 25 § 3 och 4 ska avgiftens storlek bestämmas med tillämpning av artikel 83.5 i EU:s dataskyddsförordning, i den ursprungliga lydelsen, eller, i fråga om myndigheter, med tillämpning av den högre avgiftsnivån i 6 kap. 2 § andra stycket lagen med kompletterande bestämmelser till EU:s dataskyddsförordning. Vid kamerabevakning som omfattas av brottsdatalagen ska avgiftens storlek i stället bestämmas med tillämpning av 6 kap. 3 § andra stycket den lagen.

Paragrafen, som saknar motsvarighet i kameraövervakningslagen, reglerar vilka avgiftsnivåer som ska tillämpas vid bestämmandet av en sanktionsavgift.

Av *första stycket* följer att vid överträdelser som rör lagens bestämmelser om tillståndskrav gäller den avgiftsnivå som föreskrivs i artikel 83.4 i dataskyddsförordningen för enskilda subjekt (upp till 10 000 000 EUR eller, om det gäller ett företag, upp till 2 procent av den totala globala årsomsättningen under föregående budgetår, beroende på vilket belopp som är högst). Hänvisningen till dataskyddsförordningen är statisk, dvs. avser den ursprungliga lydelsen av förordningen. För myndigheter gäller i stället den lägre avgiftsnivå som föreskrivs i 6 kap. 2 § andra stycket dataskyddslagen (högst 5 000 000 kronor). Vid kamerabevakning som omfattas av brottsdatalagen gäller i stället den avgiftsnivå som föreskrivs i 6 kap. 3 § första stycket den lagen (högst 5 000 000 kronor).

Av *andra stycket* följer att vid överträdelser som rör lagens bestämmelser om upplysningskrav gäller den avgiftsnivå som föreskrivs i artikel 83.5 i dataskyddsförordningen för enskilda subjekt (upp till 20 000 000 EUR eller, om det gäller ett företag, upp till 4 procent av den totala globala årsomsättningen under föregående budgetår, beroende på vilket belopp som är högst). Hänvisningen till dataskyddsförordningen är

statisk, dvs. avser den ursprungliga lydelsen av förordningen För myndigheter gäller i stället den högre avgiftsnivå som föreskrivs i 6 kap. 2 § andra stycket dataskyddslagen (högst 10 000 000 kronor). Vid kamerabevakning som omfattas av brottsdatalagen gäller i stället den avgiftsnivå som föreskrivs i 6 kap. 3 § andra stycket den lagen (högst 10 000 000 kronor).

Skadestånd

28 § Vid överträdelse av bestämmelser i denna lag eller av beslut som har meddelats med stöd av lagen ska bestämmelser om rätt till ersättning i artikel 82 i EU:s dataskyddsförordning tillämpas. Vid kamerabevakning som omfattas av brottsdatalagen (2018:000) ska i stället 7 kap. 1 § den lagen tillämpas.

Paragrafen, som delvis motsvarar 44 § kameraövervakningslagen, anger vilka bestämmelser om skadestånd som ska tillämpas vid överträdelser. Övervägandena finns i avsnitt 11.3.

Av paragrafen följer att regleringen i dataskyddsförordningen om rätt till ersättning ska tillämpas vid kamerabevakning som omfattas av förordningens tillämpningsområde och vid kamerabevakning som faller utanför EU-rättens tillämpningsområde. Hänvisningen till dataskyddsförordningen avser förordningen i den vid varje tidpunkt gällande lydelsen. Vid kamerabevakning som omfattas av brottsdatalagens tillämpningsområde ska regleringen om skadestånd i den lagen tillämpas i stället.

Överklagande

29 § Tillsynsmyndighetens beslut enligt denna lag får överklagas till allmän förvaltningsdomstol. När ett beslut överklagas, är tillsynsmyndigheten motpart i domstolen.

Beslut om tillstånd till kamerabevakning och om undantag enligt 20 § får överklagas även av den kommun där bevakningen ska ske och, om bevakningen ska avse en arbetsplats, av en organisation som företräder arbetstagarna på arbetsplatsen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen, som i huvudsak motsvarar 47 § kameraövervakningslagen, reglerar överklagande av beslut enligt kamerabevakningslagen. Övervägandena finns i avsnitt 11.4.

Enligt *första stycket* får tillsynsmyndighetens beslut enligt kamerabevakningslagen överklagas till allmän förvaltningsdomstol. Rätten att överklaga gäller bl.a. beslut i frågor om tillstånd till kamerabevakning och undantag från kravet på upplysning om kamerabevakning samt beslut om sanktionsavgift. När tillsynsmyndighetens beslut överklagas är den myndigheten motpart i domstolen.

Av 42 § förvaltningslagen (2017:900) framgår att ett beslut får överklagas av den som beslutet angår, om det har gått honom eller henne emot. Enligt *andra stycket* får beslut om tillstånd till kamerabevakning och om undantag enligt 20 § överklagas även av den kommun där bevakningen ska ske och, om kamerabevakningen ska avse en arbetsplats, av en organisation som företräder arbetstagarna på arbetsplatsen.

Enligt *tredje stycket* krävs prövningstillstånd vid överklagande till kammarrätten.

Ikraftträdande- och övergångsbestämmelser

1. Denna lag träder i kraft den 1 augusti 2018.
2. Genom lagen upphävs kameraövervakningslagen (2013:460).
3. Tillstånd till kameraövervakning som har beslutats enligt den upphävda lagen och som avser kamerabevakning som omfattas av kravet på tillstånd i den nya lagen gäller fortfarande. Övriga tillstånd som har beslutats enligt den upphävda lagen gäller inte längre.
4. Anmälningar som har gjorts enligt den upphävda lagen gäller inte längre.
5. Beslut om undantag från upplysningskravet som har fattats enligt 27 § tredje stycket den upphävda lagen gäller som ett beslut om undantag från upplysningskravet och rätten till information enligt 17 § den nya lagen.
6. Ärenden som har inletts hos länsstyrelserna enligt den upphävda lagen men ännu inte har avgjorts ska överlämnas till den myndighet som utövar tillsyn över kamerabevakning enligt den nya lagen.
7. Om ett beslut som har fattats enligt den upphävda lagen har överklagats av någon annan än tillsynsmyndigheten enligt den nya lagen, är tillsynsmyndigheten motpart i domstolen.
8. Äldre föreskrifter om straff gäller fortfarande för överträdelser som har skett före ikraftträdandet.

Övervägandena till ikraftträdande- och övergångsbestämmelserna finns i avsnitt 12.

Av *punkterna 1* och *2* följer att lagen träder i kraft den 1 augusti 2018 och att den äldre lagen, kameraövervakningslagen, då upphör att gälla.

Bestämmelserna i *punkterna 3* och *4* innebär att ett tillstånd till kameraövervakning som har beslutats med stöd av kameraövervakningslagen gäller även när den nya lagen har trätt i kraft, om tillståndet avser kamerabevakning som omfattas av kravet på tillstånd i den nya lagen. Övriga tillstånd som har beslutats enligt kameraövervakningslagen gäller däremot inte längre. Anmälningar som har gjorts enligt kameraövervakningslagen gäller heller inte längre.

Av *punkten 5* framgår att beslut om undantag från upplysningsplikten som har fattats med stöd av 27 § tredje stycket kameraövervakningslagen fortsätter att gälla som ett beslut om undantag från upplysningskravet och rätten till information enligt 17 § den nya lagen. Sådana äldre beslut innebär därmed dels ett undantag från upplysningskravet i den nya lagen, dels ett undantag från rätten till information, enligt tillämplig dataskyddsreglering, om den personuppgiftsbehandling som kamerabevakningen innebär.

Av *punkten 6* framgår att länsstyrelserna ska överlämna ärenden som har inletts enligt kameraövervakningslagen men som ännu inte avgjorts till den myndighet som ska utöva tillsyn över kamerabevakning enligt den nya lagen.

Av allmänna principer följer att ärenden om tillstånd till kameraövervakning eller om undantag från upplysningsplikten som har inletts hos länsstyrelserna före ikraftträdandet av kamerabevakningslagen men ännu inte har avgjorts handläggs enligt den nya lagen. Detsamma gäller för pågående mål hos domstol som avser överklagade beslut som har meddelats med stöd av kameraövervakningslagen.

Av *punkten 7* framgår att, om ett beslut som har fattats enligt den upphävda lagen har överklagats enligt kameraövervakningslagen av någon annan än tillsynsmyndigheten enligt den nya lagen, ska tillsynsmyndigheten vara motpart i domstolen. Detta utesluter inte att det samtidigt kan finnas andra motparter.

Bestämmelsen i *punkten 8* innebär att kameraövervakningslagens straffbestämmelse fortfarande gäller för gärningar som har begåtts vid kameraövervakning före den nya lagens ikraftträdande. Administrativa sanktionsavgifter bör däremot inte tas ut för en sådan överträdelse, med hänsyn till förbudet enligt 2 kap. 10 § RF mot retroaktiv straff- och skattelagstiftning.

14.2 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

32 kap.

3 § Sekretess gäller för sådan uppgift om en enskilds personliga förhållanden som har inhämtats genom *kamerabevakning* som avses i *kamerabevakningslagen (2018:000)*, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men.

Sekretessen enligt första stycket gäller hos en domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Paragrafen reglerar sekretess till skydd för uppgift om enskilds personliga förhållanden som har inhämtats genom kamerabevakning. Övervägandena finns i avsnitt 10.

Ändringen innebär att *första stycket* ändras dels genom att uttrycket kamerabevakning ersätter uttrycket kameraövervakning, dels genom att hänvisningen till kameraövervakningslagen ersätts med en hänvisning till kamerabevakningslagen.

Ikraftträdande- och övergångsbestämmelser

1. Denna lag träder i kraft den 1 augusti 2018.
2. Äldre föreskrifter gäller fortfarande för uppgift som har inhämtats före ikraftträdandet.

Övervägandena till ikraftträdande- och övergångsbestämmelserna finns i avsnitt 12.

Enligt *punkten 1* träder ändringen i kraft den 1 augusti 2018. Av *punkten 2* följer att sekretessen enligt den tidigare lydelsen av paragrafen fortfarande gäller för uppgift som har inhämtats före ikraftträdandet.

4.5.2016 SV Europeiska unionens officiella tidning L 119/1

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 åtföljа 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*

DIREKTIV

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

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 16.2,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Regionkommitténs yttrande ([1]),

i enlighet med det ordinarie lagstiftningsförfarandet ([2]), och

av följande skäl:

(1) Skyddet för fysiska personer med avseende på behandling av personuppgifter är en grundläggande rättighet. I 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) föreskrivs 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 med avseende på behandling av deras personuppgifter bör, oavsett deras medborgarskap eller hemvist, respektera deras rättigheter och grundläggande friheter, särskilt deras rätt till skydd av personuppgifter. Detta direktiv är avsett att bidra till att skapa ett område med frihet, säkerhet och rättvisa.

(3) Den snabba tekniska utvecklingen och globaliseringen har skapat nya utmaningar vad gäller skyddet av personuppgifter. Omfattningen av insamlingen och delningen av personuppgifter har ökat avsevärt. Tekniken gör det möjligt att i en aldrig tidigare skådad omfattning behandla personuppgifter i verksamheter såsom förebyggande, förhindrande, utredning, avslöjande och lagföring av brott eller verkställighet av straffrättsliga påföljder.

(4) Det fria flödet av personuppgifter mellan behöriga myndigheter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten inom unionen, samt överföringar av sådana personuppgifter till tredjeländer och internationella organisationer, bör underlättas samtidigt som en hög skyddsnivå för personuppgifter säkerställs. Denna utveckling kräver en stark och mer sammanhängande ram för skyddet av personuppgifter inom unionen, uppbackad av kraftfullt tillsynsarbete.

(5) Europaparlamentets och rådets direktiv 95/46/EG ([3]) är tillämpligt på all behandling av personuppgifter i medlemsstaterna, såväl inom den offentliga som inom den privata sektorn. Det är emellertid inte tillämpligt på behandling av personuppgifter "som utgör ett led i en verksamhet som inte omfattas av gemenskapsrätten", t.ex. verksamhet på områdena för straffrättsligt samarbete och polissamarbete.

([1]) EUT C 391, 18.12.2012, s. 127.
([2]) 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.
([3]) 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).

(6) Rådets rambeslut 2008/977/RIF [1] är tillämpligt på områdena för straffrättsligt samarbete och polissamarbete. Tillämpningsområdet för det rambeslutet begränsas till behandling av sådana personuppgifter som överförs eller görs tillgängliga mellan medlemsstaterna.

(7) Att säkerställa en enhetlig och hög skyddsnivå för fysiska personers personuppgifter och underlätta utbytet av personuppgifter mellan behöriga myndigheter i medlemsstaterna är av avgörande betydelse för att säkerställa ett effektivt straffrättsligt samarbete och polissamarbete. Därför bör skyddet för fysiska personers rättigheter och friheter i samband med behöriga myndigheters behandling av personuppgifter 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, vara likvärdigt i alla medlemsstater. Ett effektivt skydd av personuppgifter i hela unionen förutsätter att de registrerades rättigheter stärks och att skyldigheterna för dem som behandlar personuppgifter, ökar, samt likvärdiga befogenheter för att övervaka och säkerställa efterlevnaden av bestämmelserna om skydd av personuppgifter i medlemsstaterna.

(8) 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 samt om det fria flödet för personuppgifter.

(9) Med stöd av denna grund fastställs i Europaparlamentets och rådets förordning (EU) 2016/679 [2] allmänna bestämmelser om skydd av fysiska personer i samband med behandling av personuppgifter och om det fria flödet för sådana uppgifter inom unionen.

(10) I förklaring nr 21 om skydd av personuppgifter på området för straffrättsligt samarbete och polissamarbete, fogad till slutakten från den regeringskonferens som antog Lissabonfördraget, bekräftade konferensen att det med hänsyn till dessa områdens särart kan komma att bli nödvändigt att anta särskilda regler om skydd av personuppgifter och om det fria flödet av personuppgifter på områdena för straffrättsligt samarbete och polissamarbete med stöd av artikel 16 i EUF-fördraget.

(11) Det är därför lämpligt att dessa områden behandlas i ett direktiv som fastställer särskilda regler om skydd för fysiska personer i samband med behöriga myndigheters behandling av personuppgifter 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, med respekt för den särskilda karaktären hos denna verksamhet. Sådana behöriga myndigheter kan omfatta inte bara offentliga myndigheter såsom rättsliga myndigheter, polis eller andra brottsbekämpande myndigheter, utan också alla andra organ eller enheter som genom medlemsstaternas nationella rätt har anförtrotts myndighetsutövning enligt detta direktiv. Förordning (EU) 2016/679 bör tillämpas när ett sådant organ eller en sådan enhet behandlar personuppgifter för andra ändamål än de som avses i detta direktiv. Förordning (EU) 2016/679 är därför tillämplig i fall då ett organ eller en enhet samlar in personuppgifter för andra ändamål och behandlar dessa personuppgifter ytterligare för att iaktta sina rättsliga skyldigheter. Exempelvis behåller finansinstitut vissa personuppgifter som de behandlar i syfte att utreda, avslöja eller lagföra brott, och tillhandahåller dessa personuppgifter för behöriga nationella myndigheter endast i särskilda fall och i enlighet med medlemsstaternas nationella rätt. Ett organ eller en enhet som behandlar personuppgifter för sådana myndigheters räkning inom detta direktivs tillämpningsområde bör vara bundet av ett avtal eller annan rättsakt och de bestämmelser som är tillämpliga på personuppgiftsbiträden enligt detta direktiv, medan tillämpningen av förordning (EU) 2016/679 förblir opåverkad när det gäller personuppgiftsbiträdets behandling av personuppgifter som inte omfattas av detta direktivs tillämpningsområde.

(12) Polisens och andra brottsbekämpande myndigheters verksamhet är främst inriktad på att förebygga, förhindra, utreda, avslöja och lagföra brott, inbegripet polisverksamhet där man inte på förhand vet om det inträffade utgör ett brott eller inte. Sådan verksamhet kan också innefatta myndighetsutövning genom vidtagande av tvångsåtgärder vid demonstrationer, större idrottsevenemang och upplopp. Denna verksamhet omfattar också upprätthållande av lag och ordning som en uppgift som anförtros åt polisen eller andra brottsbekämpande

[1] Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (EUT L 350, 30.12.2008, s. 60).

[2] 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) (se sidan 1 i detta nummer av EUT).

myndigheter när det är nödvändigt för att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten och mot i lag skyddade grundläggande allmänna intressen som kan leda till ett brott. Medlemsstaterna får åt behöriga myndigheter anförtro andra uppgifter som inte nödvändigtvis utförs för att förebygga, förhindra, utreda, avslöja eller lagföra brott, inklusive att skydda mot och förebygga 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 förordning (EU) 2016/679.

(13) Ett brott i den mening som avses i detta direktiv bör utgöra ett självständigt begrepp i unionsrätten enligt Europeiska unionens domstols (nedan kallad *domstolen*) tolkning.

(14) Eftersom detta direktiv inte bör tillämpas på behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten, bör verksamhet som rör nationell säkerhet, verksamhet som utförs av byråer och organ som hanterar nationella säkerhetsfrågor och medlemsstaternas behandling av personuppgifter när de utför verksamhet som omfattas av del V kapitel 2 i fördraget om Europeiska unionen (EU-fördraget) inte betraktas som verksamhet som omfattas av detta direktivs tillämpningsområde.

(15) För att säkerställa en enhetlig skyddsnivå för fysiska personer genom rättsligt verkställbara rättigheter i hela unionen och undvika avvikelser som hämmar utbytet av personuppgifter mellan behöriga myndigheter, bör detta direktiv innehålla harmoniserade bestämmelser om skydd och fri rörlighet för personuppgifter som behandlas 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. Tillnärmningen av medlemsstaternas nationella rätt bör inte leda till försämringar i det personuppgiftsskydd de tillhandahåller, utan i stället ha till syfte att säkerställa en hög skyddsnivå inom unionen. Inget ska hindra medlemsstaterna från att föreskriva starkare skyddsåtgärder än dem som fastställs i detta direktiv för skyddet av den registrerades rättigheter och friheter med avseende på behöriga myndigheters behandling av personuppgifter.

(16) Detta direktiv påverkar inte tillämpningen av principen om allmänhetens rätt att få tillgång till allmänna handlingar. Enligt förordning (EU) 2016/679 får personuppgifter i allmänna handlingar som förvaras av en offentlig myndighet eller ett offentligt eller privat organ för utförande av en uppgift av allmänt intresse lämnas ut av myndigheten eller organet i enlighet med unionsrätten eller medlemsstatens nationella lagstiftning som den offentliga 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.

(17) Det skydd som ska tillhandahållas enligt detta direktiv bör tillämpas på fysiska personer, oavsett medborgarskap eller hemvist, med avseende på behandling av deras personuppgifter.

(18) 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 detta direktiv.

(19) Europaparlamentets och rådets förordning (EG) nr 45/2001 ([1]) 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 förordning (EU) 2016/679.

(20) Detta direktiv bör inte hindra medlemsstaterna från att i nationell straffprocesslagstiftning ange vilken behandling och vilka förfaranden för behandling som berörs när det gäller domstolars och andra rättsliga myndigheters behandling av personuppgifter, särskilt när det gäller personuppgifter som ingår i ett domstolsbeslut eller i protokoll avseende straffrättsliga förfaranden.

([1]) 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).

(21) Principerna för dataskydd bör gälla all information som rör en identifierad eller 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 någon 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 som kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten för behandlingen som den tekniska utvecklingen. Principerna för dataskydd 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 längre är identifierbar.

(22) 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 i allmänhetens intresse, i enlighet med unionsrätten eller medlemstaternas nationella rätt. Offentliga myndigheters begäranden om att uppgifter ska lämnas ut bör 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 om dataskydd som är tillämpliga på behandlingens ändamål.

(23) Genetiska uppgifter bör definieras som personuppgifter som rör en fysisk persons nedärvda eller förvärvade genetiska kännetecken som ger unik information om denna enskilda persons fysiologi eller hälsa och 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. Eftersom genetiska uppgifter är komplexa och känsliga finns det en stor risk för att den personuppgiftsansvarige missbrukar och återanvänder dem för olika ändamål. All diskriminering på grundval av genetiska särdrag bör i princip vara förbjuden.

(24) Personuppgifter om hälsa bör innefatta alla 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 enskilda personen som samlats in 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 personen tilldelats för att unikt identifiera den fysiska personen för hälso- och sjukvårdsändamål, uppgifter som härrör från tester eller undersökningar av en kroppsdel eller kroppssubstans, däribland genetiska uppgifter och biologiska prover, 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.

(25) Samtliga medlemsstater är anslutna till Internationella kriminalpolisorganisationen (Interpol). För att kunna fullgöra sitt uppdrag mottar, lagrar och cirkulerar Interpol personuppgifter i syfte att hjälpa behöriga myndigheter att förebygga, förhindra och bekämpa internationell brottslighet. Därför är det lämpligt att stärka samarbetet mellan unionen och Interpol genom att främja ett effektivt utbyte av personuppgifter med respekt för de grundläggande rättigheterna och friheterna vid automatiserad behandling av personuppgifter. När personuppgifter överförs från unionen till Interpol samt till länder som har delegerade medlemmar i Interpol bör detta direktiv, framför allt bestämmelserna om internationella överföringar, gälla. Detta direktiv bör inte påverka de särskilda bestämmelserna i rådets gemensamma ståndpunkt 2005/69/RIF ([2]) och rådets beslut 2007/533/RIF ([3]).

(26) Varje behandling av personuppgifter måste vara laglig, korrekt och öppen i förhållande till berörda fysiska personer och endast genomföras för särskilda lagstadgade ändamål. Detta hindrar i sig inte brottsbekämpande myndigheter från att genomföra verksamhet såsom hemliga utredningar eller videoövervakning. Sådan verksamhet kan genomföras i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa

([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).

([2]) Rådets gemensamma ståndpunkt 2005/69/RIF av den 24 januari 2005 om utbyte av vissa uppgifter med Interpol (EUT L 27, 29.1.2005, s. 61).

([3]) Rådets beslut 2007/533/RIF av den 12 juni 2007 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) (EUT L 205, 7.8.2007, s. 63).

straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, förutsatt att verksamheten har fastställts i lag och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den fysiska personens berättigade intressen. Dataskyddsprincipen om korrekt behandling är ett begrepp som är skilt från rätten till en opartisk domstol enligt artikel 47 i stadgan och rätten till en rättvis rättegång enligt artikel 6 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). 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 och relevanta för de ändamål som de behandlas för. Det bör i synnerhet säkerställas att de uppgifter som insamlats inte är orimligt omfattande och att de inte sparas längre än vad som är nödvändigt för det ändamål för vilket uppgifterna behandlas. Personuppgifter bör endast behandlas om syftet med behandlingen inte rimligen kan uppnås genom andra medel. För att säkerställa att uppgifter inte sparas längre än nödvändigt bör den personuppgiftsansvarige införa tidsfrister för radering eller för regelbunden kontroll. Medlemsstaterna bör inrätta lämpliga skyddsåtgärder för personuppgifter som lagras under längre perioder, för arkivändamål av allmänt intresse, för vetenskapliga, statistiska eller historiska ändamål.

(27) Om behöriga myndigheter ska kunna förebygga, förhindra, utreda och lagföra brott är det nödvändigt att de behandlar personuppgifter som insamlats inom ramen för förebyggande, förhindrande, utredning och lagföring av specifika brott i ett bredare sammanhang för att utveckla förståelsen för kriminell verksamhet och göra kopplingar mellan olika upptäckta brott.

(28) För att bibehålla behandlingens säkerhet och förhindra behandling som innebär en överträdelse av detta direktiv bör personuppgifter behandlas på ett sätt som säkerställer en lämplig säkerhets- och konfidentialitetsnivå samt förhindrar obehörigt tillträde till eller obehörig användning av personuppgifter och den utrustning som används för behandlingen, med beaktande av tillgänglig teknik och den tekniska utvecklingen samt genomförandekostnader i förhållande till riskerna och den typ av personuppgifter som ska skyddas.

(29) Personuppgifter bör samlas in för särskilda, uttryckligt angivna och berättigade ändamål som omfattas av detta direktivs tillämpningsområde och bör inte behandlas för andra ändamål än att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Om samma eller en annan personuppgiftsansvarig behandlar personuppgifter för ett ändamål som omfattas av detta direktiv men som inte är det ändamål som uppgifterna insamlades för, bör behandlingen vara tillåten, förutsatt att behandlingen har godkänts i enlighet med tillämpliga rättsliga bestämmelser och är nödvändig och står i proportion till det andra ändamålet.

(30) Principen om uppgifters korrekthet bör tillämpas med hänsyn till den typ av behandling det är fråga om och syftet med denna. Särskilt i domstolsförfaranden baseras utsagor som innehåller personuppgifter på fysiska personers subjektiva uppfattning, och kan inte alltid verifieras. Följaktligen bör inte korrekthetskravet röra korrektheten i en utsaga, utan endast det faktum att en viss utsaga har gjorts.

(31) Behandling av personuppgifter på områdena för straffrättsligt samarbete och polissamarbete innebär av naturliga skäl att personuppgifter om olika kategorier av registrerade behandlas. Därför är det viktigt att i tillämpliga fall och i möjligaste mån göra en klar åtskillnad mellan personuppgifter om olika kategorier av registrerade, t.ex. brottsmisstänkta, brottsdömda och brottsoffer samt andra som berörs av ett brottmål, t.ex. vittnen, personer med relevant information eller personer med kontakter eller band till brottsmisstänkta och brottsdömda. Detta bör inte hindra tillämpningen av rätten till oskuldspresumtion som garanteras i stadgan och i Europakonventionen, tolkade enligt rättspraxis från domstolen och Europeiska domstolen för de mänskliga rättigheterna.

(32) De behöriga myndigheterna bör säkerställa att personuppgifter som är felaktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga. För att säkerställa skydd för fysiska personer, korrekthet, fullständighet eller i vilken grad personuppgifterna är aktuella och tillförlitlighet i de personuppgifter som överförs eller görs tillgängliga, bör de behöriga myndigheterna i möjligaste mån föra in nödvändiga uppgifter vid all överföring av personuppgifter.

(33) När det i detta direktiv hänvisas till medlemsstaternas nationella rätt, en rättslig grund eller lagstiftningsåtgärd innebär detta inte nödvändigtvis en lagstiftningsakt antagen av ett parlament, med förbehåll för krav i den

berörda medlemsstatens konstitutionella ordning. Medlemsstaternas nationella rätt, den rättsliga grunden eller lagstiftningsåtgärden bör emellertid i dessa fall vara tydlig och precis, och dess tillämpning förutsägbar för dem som omfattas av den i enlighet med rättspraxis från domstolen och Europeiska domstolen för de mänskliga rättigheterna. Medlemsstaternas nationella rätt som reglerar behandlingen av personuppgifter inom tillämpningsområdet för detta direktiv bör åtminstone specificera målen, vilka personuppgifter som ska behandlas, behandlingens ändamål, förfarandena för att bevara personuppgifternas integritet och konfidentialitet samt förfarandena för förstöring av dem så att tillräckliga garantier mot risken för missbruk och godtycklighet ges.

(34) Behöriga myndigheters behandling av personuppgifter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott, verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, bör omfatta varje åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter som utförs i dessa syften, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, justering eller sammanförande, begränsning av behandlingen, radering eller förstöring. Framför allt bör bestämmelserna i detta direktiv gälla personuppgifter som vid tillämpningen av detta direktiv överförs till en mottagare som inte omfattas av detta direktiv. Med sådana mottagare bör avses fysiska eller juridiska personer, myndigheter, institutioner eller andra organ som den behöriga myndigheten lagligen lämnar ut personuppgifterna till. Om personuppgifter ursprungligen samlats in av en behörig myndighet för något av detta direktivs ändamål, bör förordning (EU) 2016/679 vara tillämplig på behandlingen av dessa uppgifter för andra ändamål än de som anges i detta direktiv om behandlingen är godkänd enligt unionsrätten eller nationell rätt. Framför allt bör bestämmelserna i förordning (EU) 2016/679 gälla överföring av personuppgifter för ändamål som inte omfattas av detta direktiv. Förordning (EU) 2016/679 bör gälla när personuppgifter behandlas av en mottagare som varken är eller agerar i egenskap av behörig myndighet i den mening som avses i detta direktiv och som lagligen mottagit personuppgifter av en behörig myndighet. Vid tillämpningen av detta direktiv bör medlemsstaterna också närmare kunna ange tillämpningen av bestämmelserna i förordning (EU) 2016/679 på de villkor som anges i den förordningen.

(35) För att vara laglig bör behandlingen av personuppgifter enligt detta direktiv vara nödvändig för att utföra en uppgift av allmänt intresse som en behörig myndighet ansvarar för enligt unionsrätten eller medlemsstaternas nationella rätt 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. Denna verksamhet bör omfatta skydd av intressen som är av grundläggande betydelse för den registrerade. Utförandet av uppgifterna att förebygga, förhindra, utreda, avslöja eller lagföra brott, som de behöriga myndigheterna institutionellt har tilldelats enligt lag, gör det möjligt för dem att kräva eller beordra att fysiska personer efterlever de begäranden som gjorts. I detta fall bör den registrerades samtycke, enligt definitionen i förordning (EU) 2016/679, inte utgöra en rättslig grund för behöriga myndigheters behandling av personuppgifter. Om den registrerade är skyldig att fullgöra en rättslig förpliktelse har den registrerade inte någon genuin och fri valmöjlighet, och således är det inte möjligt att betrakta den registrerades reaktion som en frivillig viljeyttring. Detta bör inte hindra medlemsstaterna från att i lag fastställa att den registrerade får tillåta behandling av sina personuppgifter vid tillämpning av detta direktiv, såsom DNA-testning inom ramen för brottsutredningar eller övervakning av var den registrerade befinner sig med elektronisk fotboja för verkställighet av straffrättsliga påföljder.

(36) Medlemsstaterna bör föreskriva att om det i den unionsrätt eller nationella rätt som är tillämplig på den överförande behöriga myndigheten fastställs särskilda villkor som under särskilda omständigheter är tillämpliga på behandlingen av personuppgifter, såsom användning av hanteringskoder, bör den överförande behöriga myndigheten informera den mottagare till vilken uppgifterna överförs om dessa villkor och om kravet att respektera dem. Sådana villkor kan till exempel innefatta ett förbud mot att överföra personuppgifter till andra mottagare eller använda dem i andra syften än de för vilka de överfördes till mottagaren eller att informera den registrerade vid en begränsning av rätten till information utan förhandsgodkännande från den överförande behöriga myndigheten. Dessa skyldigheter bör även gälla för överföringar från den överförande behöriga myndigheten till mottagare i tredjeländer eller internationella organisationer. Medlemsstaterna bör säkerställa att den överförande behöriga myndigheten inte tillämpar dessa villkor på mottagare i andra medlemsstater eller på byråer och organ som inrättats i enlighet med avdelning V kapitlen 4 och 5 i EUF-fördraget, med undantag för sådana villkor som är tillämpliga på motsvarande överföringar av uppgifter inom den medlemsstat där den behöriga myndigheten är belägen.

(37) Personuppgifter som till sin natur är särskilt känsliga med hänsyn till grundläggande rättigheter och friheter bör åtnjuta ett 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 detta direktiv inte innebär att unionen

godtar teorier som söker fastställa förekomsten av skilda människoraser. Dessa personuppgifter bör inte behandlas såvida inte behandlingen omfattas av lämpliga skyddsåtgärder för den registrerades lagstadgade rättigheter och friheter och medges i fall som är tillåtna enligt lag, eller behandlingen, om den ännu inte är tillåten enligt lag, är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan person, eller behandlingen rör uppgifter som på ett tydligt sätt har offentliggjorts av den registrerade. Lämpliga skyddsåtgärder för den registrerades rättigheter och friheter kan till exempel inbegripa möjligheten att samla in dessa uppgifter endast i samband med andra uppgifter om den berörda fysiska personen, möjligheten att säkra de insamlande uppgifterna, striktare regler om tillgång till uppgifterna för den behöriga myndighetens personal på lämpligt sätt, och förbud mot att översända sådana uppgifter. Behandling av sådana uppgifter bör även tillåtas enligt lag när den registrerade uttryckligen har gett sitt samtycke i fall där uppgiftsbehandlingen är särskilt inkräktande för honom eller henne. Den registrerades samtycke bör dock inte i sig utgöra någon rättslig grund för behöriga myndigheters behandling av sådana känsliga personuppgifter.

(38) Den registrerade bör ha rätt att inte bli föremål för ett beslut angående bedömning av personliga aspekter rörande honom eller henne som uteslutande grundas på automatiserad behandling och som har negativa rättsliga följder eller i betydande grad påverkar honom eller henne. Denna form av uppgiftsbehandling bör under alla omständigheter omfattas av lämpliga skyddsåtgärder, inbegripet skild information till den registrerade och rätt till personlig kontakt, särskilt för framförande av egna synpunkter, rätten att erhålla en förklaring för det beslut som fattats efter sådan bedömning och rätten att överklaga beslutet. Profilering som leder till diskriminering av fysiska personer på grundval av personuppgifter som till sin natur är särskilt känsliga med hänsyn till grundläggande rättigheter och friheter är förbjuden på de villkor som fastställs i artiklarna 21 och 52 i stadgan.

(39) För att den registrerade ska kunna utöva sina rättigheter bör all information till denne vara lättåtkomlig, t.ex. via den personuppgiftsansvariges webbplats, och lättbegriplig, på ett klart och tydligt språk. Denna information bör anpassas till de behov som sårbara människor, t.ex. barn, har.

(40) Det bör finnas arrangemang som underlättar för registrerade att utöva sina rättigheter enligt de bestämmelser som antas i enlighet med detta direktiv, bl.a. rutiner för att kostnadsfritt begära och i tillämpliga fall få, särskilt, kostnadsfri tillgång till och rättelse eller radering av personuppgifter och begränsning av behandlingen. Personuppgiftsansvariga bör vara skyldiga att besvara en begäran från den registrerade utan onödigt dröjsmål, om inte de personuppgiftsansvariga tillämpar begränsningar av den registrerades rättigheter i enlighet med detta direktiv. Om en begäran är uppenbart ogrundad eller orimlig, som i fall då en registrerad utan skäl och vid upprepade tillfällen begär uppgifter eller om denne missbrukar sin rätt till information genom att exempelvis i sin begäran tillhandahålla felaktig eller missvisande information, bör den personuppgiftsansvarige dessutom kunna ta ut en rimlig avgift eller vägra att tillmötesgå begäran.

(41) När den personuppgiftsansvarige begär att ytterligare information som är nödvändig för att bekräfta den registrerades identitet ska tillhandahållas bör denna information endast behandlas för detta specifika ändamål och bör inte lagras längre än vad som krävs för detta ändamål.

(42) Åtminstone följande information bör göras tillgänglig för den registrerade: Vem som är personuppgiftsansvarig, att behandling sker, syftena med behandlingen, rätten att lämna in klagomål och rätten att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandlingen. Informationen kan anges på den behöriga myndighetens webbplats. Dessutom bör den registrerade, i specifika fall och för att göra det möjligt för honom eller henne att utöva sina rättigheter, informeras om behandlingens rättsliga grund och om hur länge uppgifterna kommer att lagras, i den utsträckning som den ytterligare informationen är nödvändig, med beaktande av de särskilda omständigheter under vilka personuppgifterna behandlas, för att garantera en korrekt behandling när det gäller den registrerade.

(43) Fysiska personer bör ha rätt att få tillgång till uppgifter som insamlats som rör dem samt att på enkelt sätt och med rimliga intervall kunna utöva denna rätt för att hålla sig underrättade om att behandling sker och kunna kontrollera att den är laglig. Därför bör varje registrerad ha rätt att känna till och underrättas om de ändamål för vilka uppgifterna behandlas, hur länge behandlingen kommer att pågå och vilka som kommer att få del av uppgifterna, inbegripet mottagare i tredjeländer. Om denna underrättelse omfattar information om personuppgifternas ursprung bör denna information inte avslöja fysiska personers identitet, framför allt konfidentiella källor. För att denna rättighet ska respekteras är det tillräckligt att den registrerade innehar en komplett sammanfattning av dessa uppgifter i begripligt format, det vill säga ett format som gör det möjligt för den registrerade att få kännedom om dessa uppgifter och kontrollera att de är korrekta och behandlade i enlighet med detta direktiv så

att den sökande kan utöva de rättigheter som han eller hon tilldelas enligt detta direktiv. En sådan sammanfattning skulle kunna tillhandahållas i form av en kopia av de personuppgifter som håller på att behandlas.

(44) Medlemsstaterna bör ha möjlighet att genom lagstiftning vidta åtgärder som innebär att informationen till de registrerade senareläggs, begränsas eller utelämnas eller att deras tillgång till sina personuppgifter helt eller delvis begränsas, i den utsträckning och så länge som en sådan åtgärd utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, och syftet är att undvika att hindra officiella eller rättsliga utredningar, undersökningar eller förfaranden, undvika menlig inverkan på förebyggande, förhindrande, utredning, upptäckt eller lagföring av brott eller verkställighet av straffrättsliga påföljder, skydd för allmän eller nationell säkerhet eller skydd för andra personers rättigheter och friheter. Den personuppgiftsansvarige bör genom en konkret och individuell granskning i varje enskilt fall bedöma om rätten till tillgång delvis eller helt bör begränsas.

(45) En vägran eller begränsning av tillgång bör i princip meddelas den registrerade skriftligen och inkludera de faktiska eller rättsliga skäl som beslutet grundar sig på.

(46) All begränsning av den registrerades rättigheter måste vara förenlig med stadgan och med Europakonventionen, tolkade enligt rättspraxis från domstolen respektive Europeiska domstolen för de mänskliga rättigheterna, och i synnerhet respektera kärnan i dessa rättigheter och friheter.

(47) Fysiska personer bör ha rätt att få felaktiga personuppgifter som rör dem rättade, särskilt faktauppgifter, samt rätt att få dem raderade om behandlingen av uppgifterna utgör en överträdelse av detta direktiv. Rätten till rättelse bör emellertid inte påverka exempelvis innehållet i ett vittnesmål. En fysisk person bör också ha rätt till begränsning av behandlingen när han eller hon bestrider korrektheten av en personuppgift och det inte kan fastställas huruvida denna är korrekt eller när personuppgiften måste sparas som bevisning. Framför allt bör behandlingen av personuppgifter begränsas snarare än att uppgifterna raderas om det i ett visst fall finns rimliga skäl att anta att en radering skulle kunna påverka den registrerades legitima intressen. I ett sådant fall bör begränsade uppgifter endast behandlas för det ändamål som hindrade att de raderades. Behandling av personuppgifter kan exempelvis begränsas genom att man flyttar de valda uppgifterna till ett annat databehandlingssystem, till exempel för arkivering, eller gör de valda uppgifterna otillgängliga. I automatiserade register bör begränsningen av behandlingen i princip ske med tekniska medel. Att behandlingen av personuppgifter är begränsad bör anges inom systemet på sådant sätt att det tydligt framgår att behandlingen av personuppgifterna är begränsad. Sådan rättelse, radering av personuppgifter eller begränsning av behandlingen bör meddelas till de mottagare till vilka uppgifterna har lämnats ut och till de behöriga myndigheter från vilka de oriktiga uppgifterna härrörde. De personuppgiftsansvariga bör också avstå från vidare spridning av sådana uppgifter.

(48) Om en personuppgiftsansvarig nekar en registrerad dennes rätt till information, tillgång till, rättelse, eller radering av personuppgifter eller till begränsning av behandlingen bör den registrerade ha rätt att begära att den nationella tillsynsmyndigheten kontrollerar behandlingens laglighet. De registrerade bör informeras om denna rättighet. När en tillsynsmyndighet agerar för de registrerades räkning, bör tillsynsmyndigheten åtminstone informera dem om att tillsynsmyndigheten har utfört alla nödvändiga kontroller eller översyner. Tillsynsmyndigheten bör också informera de registrerade om rätten att begära rättslig prövning.

(49) När personuppgifter behandlas inom ramen för en brottsutredning eller domstolsförfaranden vid brottmål, bör medlemsstaterna kunna föreskriva att rätten till information, tillgång, rättelse och radering samt till begränsning av behandlingen utövas i enlighet med nationella bestämmelser om rättsliga förfaranden.

(50) Den personuppgiftsansvarige 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 bör kunna visa att behandlingen är förenlig med detta direktiv. I samband med dessa åtgärder bör behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter beaktas. De åtgärder som den personuppgiftsansvarige vidtar bör omfatta utarbetande och genomförande av särskilda skyddsåtgärder för behandling av personuppgifter om sårbara fysiska personer, t.ex. barn.

(51) Risker för fysiska personers rättigheter och friheter, av varierande sannolikhetsgrad och allvar, kan uppkomma till följd av uppgiftsbehandling som skulle kunna medföra fysiska, materiella eller immateriella skador, i synnerhet om behandlingen kan leda till diskriminering, identitetsstöld eller identitetsbedrägeri, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller uppgifter som omfattas av tystnadsplikt, obehörigt hävande av

pseudonymisering, eller annan betydande ekonomisk eller social nackdel; eller om registrerade kan komma att 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 eller biometriska uppgifter behandlas för att unikt identifiera en person eller om uppgifter om hälsa eller uppgifter om sexualliv och sexuell läggning eller fällande domar i brottmål samt brott eller därmed sammanhängande säkerhetsåtgärder behandlas; om det förekommer en bedömning av personliga aspekter, exempelvis analyser och 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; eller om personuppgifter rörande sårbara fysiska personer, framför allt barn, behandlas; eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.

(52) Riskens sannolikhetsgrad och allvar bör fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål. Risken bör utvärderas enligt en objektiv bedömning, genom vilken det fastställs huruvida uppgiftsbehandlingen medför hög risk. Med hög risk avses en särskild risk för menlig inverkan på registrerades rättigheter och friheter.

(53) Skyddet för fysiska personers rättigheter och friheter i samband med behandlingen av personuppgifter kräver lämpliga tekniska och organisatoriska åtgärder för att säkerställa att kraven i detta direktiv uppfylls. Genomförandet av sådana åtgärder bör inte enbart bero på ekonomiska hänsyn. För att kunna visa överensstämmelse med detta direktiv bör den personuppgiftsansvarige anta interna strategier och vidta åtgärder, som i synnerhet följer principerna om inbyggt dataskydd och dataskydd som standard. Om den personuppgiftsansvarige har genomfört en konsekvensbedömning avseende dataskydd i enlighet med detta direktiv bör resultatet beaktas vid utarbetandet av dessa åtgärder och förfaranden. Sådana åtgärder kan bland annat bestå av pseudonymisering snarast möjligt. Pseudonymisering vid tillämpning av detta direktiv kan utgöra ett verktyg som kan underlätta det fria flödet av personuppgifter inom området med frihet, säkerhet och rättvisa.

(54) Skyddet för de registrerades rättigheter och friheter samt de personuppgiftsansvarigas och registerförarnas ansvar, också i förhållande till tillsynsmyndigheternas övervakning och åtgärder, kräver ett tydligt fastställande av vem som bär ansvaret enligt detta direktiv, 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.

(55) Ett personuppgiftsbiträdes behandling bör styras av en rättsakt som omfattar ett avtal som binder personuppgiftsbiträdet till den personuppgiftsansvarige och där det särskilt anges att personuppgiftsbiträdet endast bör agera på instruktion av den personuppgiftsansvarige. Personuppgiftsbiträdet bör beakta principen om inbyggt dataskydd och dataskydd som standard.

(56) För att visa överensstämmelse med detta direktiv bör de personuppgiftsansvariga eller registerförarna föra register över alla kategorier av 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 för myndigheten så att det kan tjäna som grund för övervakningen av behandlingen. Personuppgiftsansvariga eller personuppgiftsbiträden som behandlar personuppgifter i icke-automatiserade behandlingssystem bör ha infört effektiva metoder, t.ex. loggar eller andra typer av register, för att visa att behandlingen är laglig, möjliggöra egenkontroll och säkerställa dataintegritet och datasäkerhet.

(57) Loggar bör åtminstone föras över behandlingar i automatiserade behandlingssystem såsom insamling, ändring, läsning, utlämning, inklusive överföringar, sammanförande eller radering. Identifieringen av den person som läst eller lämnat ut personuppgifter bör loggas och från denna identifiering skulle det kunna vara möjligt att fastställa motiveringen till behandlingen. Loggarna bör endast användas för att kontrollera om behandlingen av uppgifterna är tillåten, för egenkontroll, för att garantera dataintegritet och datasäkerhet samt för straffrättsliga förfaranden. Egenkontroll omfattar även behöriga myndigheters interna disciplinära förfaranden.

(58) En konsekvensbedömning avseende dataskydd bör genomföras av den personuppgiftsansvarige om det är sannolikt att uppgiftsbehandlingen, på grund av sin karaktär, sin omfattning eller sina ändamål, medför en hög risk för de registrerades rättigheter och friheter, vilken i synnerhet bör omfatta planerade åtgärder, skyddsåtgärder och mekanismer för att säkerställa skyddet av personuppgifter och för att styrka efterlevnaden av detta direktiv. Konsekvensbedömningarna bör omfatta relevanta system och processer för behandling men inte enskilda fall.

(59) I syfte att säkerställa ett effektivt skydd av de registrerades rättigheter och friheter bör den personuppgiftsansvarige eller personuppgiftsbiträdet i vissa fall samråda med tillsynsmyndigheten före behandlingen.

(60) För att upprätthålla säkerheten och förhindra behandling som bryter mot detta direktiv bör personuppgiftsansvariga eller personuppgiftsbiträden utvärdera de risker som behandlingen är förknippad med och bör vidta åtgärder, såsom kryptering, för att mildra dem. Åtgärderna bör leda till en lämplig säkerhetsnivå, inklusive konfidentialitetsnivå, med beaktande av den senaste utvecklingen och till genomförandekostnaderna med hänsyn till riskerna och vilken typ av personuppgifter som ska skyddas. Vid bedömningen av riskerna när det gäller datasäkerhet bör man beakta de risker som uppgiftsbehandling medför, såsom förstöring, förlust eller ändringar genom olyckshändelse eller olagliga handlingar eller obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats, som framför allt kan leda till fysisk, materiell eller immateriell skada. Den personuppgiftsansvarige och personuppgiftsbiträdet bör säkerställa att behandlingen av personuppgifter inte utförs av obehöriga personer.

(61) 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 identitetsbedrägeri, ekonomisk förlust, obehörigt hävande av pseudonymisering, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, eller till annan betydande ekonomisk eller social nackdel för den berörda fysiska personen. Så snart en personuppgiftsansvarig blir medveten om en personuppgiftsincident bör den personuppgiftsansvarige därför anmäla personuppgiftsincidenten till tillsynsmyndigheten utan onödigt dröjsmål och, om möjligt, inom 72 timmar efter att ha fått kännedom om denna, om inte den personuppgiftsansvarige, i enlighet med ansvarsprincipen, kan visa att det är osannolikt att personuppgiftsincidenten kommer att medföra en risk för fysiska personers rättigheter och friheter. Om anmälan inte kan göras inom 72 timmar bör skälen till fördröjningen åtföljа anmälan och informationen får lämnas i omgångar utan otillbörligt vidare dröjsmål.

(62) Fysiska personer bör utan onödigt dröjsmål underrättas om personuppgiftsincidenten sannolikt leder till en högre risk för deras rättigheter och friheter så att de kan vidta nödvändiga försiktighetsåtgärder. Underrättelsen bör innehålla en beskrivning av personuppgiftsincidentens art samt rekommendationer till 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 kräver behovet av att mildra en omedelbar skaderisk att de registrerade underrättas omgående medan behovet att vidta lämpliga åtgärder vid fortlöpande eller likartade uppgiftsincidenter kan motivera längre tid för underrättelsen. Om man inte kan undvika att hindra officiella eller rättsliga utredningar, undersökningar eller förfaranden, undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder eller skydda allmän säkerhet, nationell säkerhet eller andra personers rättigheter och friheter genom att senarelägga eller begränsa informationen till den berörda fysiska personen om en personuppgiftsincident skulle denna information under exceptionella omständigheter kunna utelämnas.

(63) Den personuppgiftsansvarige bör utse en person att hjälpa denne att övervaka den interna efterlevnaden av de bestämmelser som antas i enlighet med detta direktiv, förutom om en medlemsstat beslutar att undanta domstolar och andra oberoende rättsliga myndigheter som behandlar personuppgifter inom ramen för sin dömande verksamhet. Denna person kan vara en av den personuppgiftsansvariges medarbetare som fått särskild utbildning inom dataskyddslagstiftning och praxis i fråga om dataskydd för att förvärva sakkunskap på detta område. Den nödvändiga nivån på sakkunskapen bör särskilt fastställas i enlighet med den uppgiftsbehandling som utförs och det skydd som krävs för de personuppgifter som behandlas av den personuppgiftsansvarige. Hans eller hennes uppgift kan utföras på deltid eller heltid. Flera personuppgiftsansvariga kan, med beaktande av organisationsstruktur och storlek, gemensamt utse ett dataskyddsombud, t.ex. vid gemensamma resurser i centralenheter. Denna person kan också utnämnas till olika befattningar inom de berörda personuppgiftsansvarigas struktur. Denna person bör hjälpa den personuppgiftsansvarige och de anställda som behandlar personuppgifter genom att ge information och råd till dem angående efterlevnaden av deras respektive skyldigheter i fråga om dataskydd. Dataskyddsombudet i fråga bör kunna utföra sina uppdrag och uppgifter på ett oberoende sätt i enlighet med medlemsstaternas nationella rätt.

(64) Medlemsstaterna bör säkerställa att överföringar till ett tredjeland eller en internationell organisation endast får äga rum om detta är nödvändigt för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller för att verkställa straffrättsliga påföljder, inklusive för att skydda mot samt förebygga och förhindra hot mot den

allmänna säkerheten, och den personuppgiftsansvarige i tredjelandet eller den internationella organisationen är en myndighet som är behörig i den mening som avses i detta direktiv. En överföring bör endast utföras av behöriga myndigheter som agerar som personuppgiftsansvariga, utom när personuppgiftsbiträden uttryckligen har getts i uppdrag att göra en överföring för personuppgiftsansvarigas räkning. En sådan överföring kan äga rum när kommissionen har beslutat att skyddsnivån i ett tredjeland eller en internationell organisation är adekvat eller när lämpliga skyddsåtgärder föreligger, eller när undantag för särskilda situationer gäller. Det är viktigt att den skyddsnivå som fysiska personer garanteras inom unionen genom detta direktiv inte undergrävs när personuppgifter överförs från unionen till personuppgiftsansvariga, personuppgiftsbiträden eller andra mottagare i tredjeländer eller internationella organisationer, vilket inbegriper fall av vidare överföring av personuppgifter från tredjelandet eller den internationella organisationen till personuppgiftsansvariga eller personuppgiftsbiträden i samma eller i ett annat tredjeland eller en annan internationell organisation.

(65) Om personuppgifter överförs från en medlemsstat till tredjeländer eller internationella organisationer bör en sådan överföring i princip ske först efter det att den medlemsstat från vilken uppgifterna insamlades har gett sitt tillstånd till överföringen. För ett effektivt samarbete i fråga om brottsbekämpning krävs att, om ett hot mot en medlemsstats eller ett tredjelands allmänna säkerhet eller en medlemsstats väsentliga intressen är så överhängande att det är omöjligt att i tid inhämta ett förhandstillstånd, den behöriga myndigheten bör få överföra de relevanta personuppgifterna till det berörda tredjelandet eller internationella organisationen utan sådant förhandstillstånd. Medlemsstaterna bör föreskriva att eventuella särskilda villkor som rör överföringen bör vidarebefordras till tredjeländer eller internationella organisationer. För vidare överföring av personuppgifter bör det krävas förhandstillstånd från den behöriga myndighet som utförde den ursprungliga överföringen. När den behöriga myndighet som utförde den ursprungliga överföringen fattar beslut om en begäran om tillstånd för vidare överföring bör den vederbörligen beakta alla relevanta faktorer, inklusive hur allvarligt brottet är, de särskilda villkor på vilka, och det ändamål för vilket, uppgifterna ursprungligen överfördes, arten och villkoren för verkställandet av den straffrättsliga påföljden, samt nivån på skyddet av personuppgifter i det tredjeland eller den internationella organisation som personuppgifterna vidare överförs till. Den behöriga myndighet som utförde den ursprungliga överföringen bör också ha möjlighet att tillämpa särskilda villkor för vidare överföring. Dessa särskilda villkor kan beskrivas, t.ex. i hanteringskoder.

(66) Kommissionen bör med verkan för hela unionen kunna fastställa att vissa tredjeländer, ett visst territorium eller en eller flera specificerade sektorer i ett tredjeland eller en internationell organisation kan erbjuda en adekvat dataskyddsnivå, och på så sätt skapa rättssäkerhet och enhetlighet i hela unionen vad gäller dessa tredjeländer eller internationella organisationer som anses erbjuda en sådan skyddsnivå. I dessa fall bör överföringar av personuppgifter till dessa länder kunna ske utan särskilt tillstånd, utom när en annan medlemsstat från vilken uppgifterna insamlades måste ge tillstånd till överföringen.

(67) I enlighet med de grundläggande värderingar som unionen vilar på, särskilt skyddet av de mänskliga rättigheterna, bör kommissionen i sin bedömning av ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland beakta i vilken omfattning ett visst tredjeland iakttar rättsstatsprincipen, möjligheten till rättslig prövning samt internationella människorättsliga normer och standarder samt landets allmänna lagstiftning och sektorslagstiftning, vilket inbegriper 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 det tredjelandet. Tredjelandet bör erbjuda garantier som säkerställer en tillfredsställande skyddsnivå, som i huvudsak motsvarar den som säkerställs inom unionen, i synnerhet när uppgifter behandlas inom en eller flera specifika sektorer. Tredjelandet bör framför allt säkerställa en effektiv oberoende dataskyddsövervakning samt sörja för mekanismer för samarbete med medlemsstaternas dataskyddsmyndigheter och de registrerade bör tillförsäkras effektiva och verkställbara rättigheter samt effektiva administrativa och rättsliga rättsmedel.

(68) Utöver de internationella åtaganden som tredjelandet eller den internationella organisationen har ingått bör kommissionen också beakta de skyldigheter som följer av tredjelandets eller den internationella organisationens deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter, samt genomförandet av dessa skyldigheter. Framför allt bör tredjelandets anslutning till Europarådets konvention av den 28 januari 1981 om skydd för fysiska personer vid automatiserad databehandling av personuppgifter och dess tilläggsprotokoll beaktas. Kommissionen bör samråda med Europeiska dataskyddsstyrelsen, inrättad genom förordning

(EU) 2016/679 (nedan kallad *styrelsen*) vid bedömningen av skyddsnivån i tredjeländer eller internationella organisationer. Kommissionen bör också beakta alla relevanta kommissionsbeslut om adekvat skyddsnivå som antagits i enlighet med artikel 45 i förordning (EU) 2016/679.

(69) Kommissionen bör övervaka hur beslut om skyddsnivå i ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland eller en internationell organisation fungerar. I sina beslut om adekvat skyddsnivå bör kommissionen föreskriva en mekanism för periodisk översyn av hur de fungerar. Denna periodiska översyn bör göras i samråd med tredjelandet eller den internationella organisationen i fråga och bör beakta all relevant utveckling i tredjelandet eller den internationella organisationen.

(70) Kommissionen bör även kunna konstatera att ett tredjeland eller ett territorium eller en specificerad sektor inom ett tredjeland, eller en internationell organisation, inte längre säkerställer en adekvat dataskyddsnivå. Följaktligen bör överföringar av personuppgifter till det tredjelandet eller den internationella organisationen förbjudas om inte kraven i detta direktiv rörande överföring som är föremål för lämpliga skyddsåtgärder och undantag i särskilda situationer är uppfyllda. Bestämmelser bör fastställas för förfaranden för 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.

(71) Överföringar som inte grundar sig på ett sådant beslut om adekvat skyddsnivå bör endast tillåtas om lämpliga skyddsåtgärder garanteras i ett rättsligt bindande instrument, som säkerställer skyddet av personuppgifterna eller om den personuppgiftsansvarige har gjort en bedömning av alla omständigheter kring en uppgiftsöverföring och på grundval av denna bedömning anser att lämpliga skyddsåtgärder föreligger vad avser skyddet av personuppgifter. Sådana rättsligt bindande instrument kan t.ex. vara rättsligt bindande bilaterala avtal som har ingåtts av medlemsstaterna och genomförts inom deras rättsordning och som kan åberopas av registrerade som omfattas av denna och som sörjer för att kraven i fråga om dataskydd uppfylls och att registrerades rättigheter respekteras, inbegripet rätten till en effektiv administrativ eller rättslig prövning. Den personuppgiftsansvarige bör vid bedömningen av alla omständigheter kring uppgiftsöverföringen kunna beakta samarbetsavtal som ingåtts mellan Europol eller Eurojust och tredjeländer, som medger utbyte av personuppgifter. Den personuppgiftsansvarige bör också kunna beakta att överföringen av personuppgifter kommer att omfattas av tystnadplikt och principen om specificitet, vilket säkerställer att personuppgifterna inte kommer att behandlas i andra syften än för överföringen. Dessutom bör den personuppgiftsansvarige beakta att personuppgifterna inte kommer att användas för att göra framställningar om, meddela eller verkställa dödsstraff eller någon form av grym och omänsklig behandling. Även om dessa villkor kan betraktas som tillräckliga skyddsåtgärder för överföringen av uppgifter bör den personuppgiftsansvarige kunna begära ytterligare skyddsåtgärder.

(72) Om det inte finns något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder saknas kan en överföring eller en kategori av överföringar endast äga rum i särskilda situationer om överföringen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan person, eller för att skydda den registrerades berättigade intressen om lagstiftningen i den medlemsstat som överför personuppgifterna föreskriver detta, eller för att avvärja ett omedelbart och allvarligt hot mot den allmänna säkerheten i en medlemsstat eller i ett tredjeland, eller om det är nödvändigt i ett enskilt fall för att förebygga, förhindra, avslöja, utreda eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive för att skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten, eller i ett enskilt fall för att fastslå, göra gällande eller försvara rättsliga anspråk. Dessa undantag bör tolkas restriktivt och bör inte möjliggöra upprepade, omfattande eller strukturella överföringar av personuppgifter eller storskaliga överföringar av uppgifter, utan begränsas till uppgifter som är absolut nödvändiga. Sådana överföringar bör dokumenteras och på begäran göras tillgängliga för tillsynsmyndigheten så att man kan övervaka om överföringen är laglig.

(73) Medlemsstaternas behöriga myndigheter tillämpar gällande bilaterala eller multilaterala internationella avtal som ingåtts med tredjeländer på området för straffrättsligt samarbete och polissamarbete för utbyte av relevant information för att de ska kunna fullgöra de uppgifter som de anförtrotts enligt lag. Detta sker i princip genom eller åtminstone i samarbete med tredjeländernas berörda myndigheter, i vissa fall även i avsaknad av ett bilateralt eller multilateralt internationellt avtal. I specifika enskilda fall är emellertid de ordinarie förfaranden som kräver kontakt med myndigheten i tredjelandet ineffektiva eller olämpliga, framför allt för att överföringen inte skulle kunna utföras i tid eller för att myndigheten i tredjelandet inte respekterar rättsstatsprincipen eller internationella människorättsliga normer och standarder, så att medlemsstaternas behöriga myndigheter skulle kunna besluta att överföra personuppgifterna direkt till de mottagare som är etablerade i dessa tredjeländer. Detta kan till exempel vara fallet om det finns ett akut behov av att överföra personuppgifter för att rädda livet på en person som riskerar att utsättas för ett brott eller för att förhindra en överhängande fara för brottslighet, inbegripet terrorism. Även om denna överföring mellan behöriga myndigheter och mottagare som är etablerade i tredjeländer endast

äger rum i särskilda enskilda fall bör det i detta direktiv föreskrivas villkor för att reglera sådana fall. Dessa bestämmelser bör inte betraktas som undantag från något befintligt bilateralt eller multilateralt internationellt avtal på området för straffrättsligt samarbete och polissamarbete. Dessa bestämmelser bör vara tillämpliga utöver övriga bestämmelser i detta direktiv, särskilt bestämmelserna om när personuppgifter får behandlas och bestämmelserna i kapitel V.

(74) När personuppgifter förs över gränserna kan detta öka risken för att fysiska personer inte ska kunna utöva sina dataskyddsrättigheter för att skydda sig mot olaglig användning eller olagligt utlämnande av dessa uppgifter. Samtidigt kan tillsynsmyndigheter finna att de inte är i stånd att handlägga klagomål eller genomföra utredningar avseende verksamheter utanför sina egna gränser. Deras strävan att samarbeta i ett gränsöverskridande sammanhang kan också försvåras på grund av otillräckliga preventiva eller korrigerande befogenheter och oenhetliga rättsliga regelverk. Närmare samarbete mellan tillsynsmyndigheter bör därför främjas för att hjälpa dem att utbyta information med sina utländska motparter.

(75) För att skydda fysiska personer med avseende på behandling av personuppgifter är det av avgörande betydelse att medlemsstaterna inrättar tillsynsmyndigheter som kan utföra sitt uppdrag fullständigt oberoende. Tillsynsmyndigheterna bör övervaka tillämpningen av detta direktiv och bör bidra till enhetlig tillämpning av dessa i hela unionen, för att skydda fysiska personer när deras personuppgifter behandlas. För detta ändamål bör tillsynsmyndigheterna samarbeta såväl sinsemellan som med kommissionen.

(76) Medlemsstaterna får anförtro en tillsynsmyndighet som de redan har inrättat i enlighet med förordning (EU) 2016/679 ansvaret för de uppgifter som ska utföras av de nationella tillsynsmyndigheter som ska inrättas i enlighet med detta direktiv.

(77) Medlemsstaterna bör kunna inrätta mer än en tillsynsmyndighet för att återspegla sin konstitutionella, organisatoriska och administrativa struktur. Varje tillsynsmyndighet bör tilldelas de ekonomiska och personella resurser och lokalutrymmen samt den infrastruktur som krävs 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.

(78) Tillsynsmyndigheterna bör vara föremål för oberoende kontroll- eller övervakningsmekanismer i fråga om sina utgifter, förutsatt att denna finansiella kontroll inte påverkar deras oberoende.

(79) De allmänna villkoren för tillsynsmyndighetens ledamot eller ledamöter bör fastställas i medlemsstaternas nationella rätt och bör i synnerhet föreskriva att de ska utnämnas antingen av den berörda medlemsstatens parlament eller dess regering eller dess statschef på grundval av ett förslag från regeringen eller en minister eller parlamentet eller dess kammare eller av ett oberoende organ som enligt medlemsstaternas nationella rätt har anförtrotts utnämningen genom ett öppet förfarande. I syfte att säkerställa tillsynsmyndighetens oberoende bör ledamoten eller ledamöterna handla med integritet, bör 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. För att säkerställa tillsynsmyndighetens oberoende bör personalurvalet göras av tillsynsmyndigheten, och kunna innefatta ett ingripande från ett oberoende organ som enligt medlemsstaternas nationella rätt har anförtrotts uppgiften.

(80) Detta direktiv är visserligen tillämpligt på nationella domstolars och andra rättsliga myndigheters verksamheter, men tillsynsmyndigheterna bör inte ha behörighet att övervaka behandling av personuppgifter inom ramen för domstolars dömande verksamhet. Syftet är att garantera domarnas oberoende när de utför sina rättsliga uppgifter. Detta undantag bör vara inskränkt till rättsliga verksamheter i domstolsmål och inte vara tillämpligt på övriga verksamheter där domare i enlighet med medlemsstaternas nationella rätt kan medverka. Medlemsstaterna bör också kunna föreskriva att tillsynsmyndigheten inte ska vara behörig att övervaka andra oberoende rättsliga myndigheter som behandlar personuppgifter inom ramen för sin rättsliga verksamhet, exempelvis allmänna åklagarmyndigheter. Under alla omständigheter är domstolarnas och andra oberoende rättsliga myndigheters efterlevnad av bestämmelserna i detta direktiv alltid föremål för en oberoende kontroll i enlighet med artikel 8.3 i stadgan.

(81) Tillsynsmyndigheterna bör hantera klagomål som anförs av registrerade och utreda ärendena i fråga eller överföra dem till den behöriga övervakande myndigheten. Utredningen av ett klagomål bör, med förbehåll för eventuell domstolsprövning, ske i den utsträckning som är lämplig i det enskilda fallet. Tillsynsmyndigheten bör i rimlig tid informera den registrerade om hur arbetet med klagomålet fortskrider och vad resultatet blir. Om ärendet kräver ytterligare utredning eller samordning med en annan tillsynsmyndighet bör den registrerade underrättas även om detta.

(82) För att man ska kunna övervaka efterlevnaden av och verkställa detta direktiv på ett effektivt, tillförlitligt och enhetligt sätt i hela unionen enligt EUF-fördraget, i enlighet med den tolkning som domstolen gjort, bör tillsynsmyndigheterna i alla medlemsstater ha samma uppgifter och effektiva befogenheter, bl.a. undersökningsbefogenheter, korrigerande befogenheter och rådgivande befogenheter, som utgör nödvändiga medel för utförandet av deras uppgifter. Emellertid bör deras befogenheter inte inkräkta på särskilda regler för straffrättsliga förfaranden, inbegripet utredning och lagföring av brott, eller domstolsväsendets oberoende. Utan att det påverkar åklagarmyndigheternas befogenheter enligt medlemsstaternas nationella rätt bör tillsynsmyndigheterna också ha befogenhet att upplysa de rättsliga myndigheterna om överträdelser av detta direktiv eller delta i rättsliga förfaranden. Tillsynsmyndigheternas befogenheter bör utövas i överensstämmelse med lämpliga rättssäkerhetsgarantier som fastställs i unionsrätten och i medlemsstaternas nationella rätt samt opartiskt, korrekt och inom rimlig tid. Framför allt bör varje åtgärd vara lämplig, nödvändig och proportionell för att säkerställa efterlevnaden av detta direktiv, med beaktande av omständigheterna i varje enskilt fall, samt respektera varje persons rätt att bli hörd innan några enskilda åtgärder som påverkar den berörda personen negativt vidtas, och utformas så att onödiga kostnader och alltför stora olägenheter för denne undviks. Undersökningsbefogenheten när det gäller tillträde till lokaler bör utövas i enlighet med särskilda krav i medlemsstaternas nationella rätt, såsom kravet på att inhämta förhandstillstånd från rättsliga myndigheter. Antagande av ett rättsligt bindande beslut bör bli föremål för domstolsprövning i den medlemsstat där den tillsynsmyndighet som antog beslutet är belägen.

(83) Tillsynsmyndigheterna bör bistå varandra när de utför sina uppgifter och ge ömsesidigt bistånd för att säkerställa att de bestämmelser som antas i enlighet med detta direktiv efterlevs och tillämpas på ett enhetligt sätt.

(84) Styrelsen bör bidra till detta direktivs enhetliga tillämpning i hela unionen, bl.a. genom att lämna råd till kommissionen och främja samarbetet mellan tillsynsmyndigheterna i hela unionen.

(85) Alla registrerade bör ha rätt att lämna in ett klagomål till en enda tillsynsmyndighet och till ett effektivt rättsmedel i enlighet med artikel 47 i stadgan, om den registrerade anser att hans eller hennes rättigheter enligt de bestämmelser som antas i enlighet med detta direktiv 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. Den behöriga tillsynsmyndigheten bör i rimlig tid informera den registrerade om hur arbetet med klagomålet fortskrider och vad resultatet blir. Om ärendet kräver ytterligare utredning eller samordning med en annan tillsynsmyndighet bör den registrerade underrättas även om detta. För att förenkla inlämnandet 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.

(86) Varje fysisk eller juridisk person bör ha rätt till ett effektivt rättsmedel vid behörig nationell domstol mot en tillsynsmyndighets beslut som har rättsliga följder för denna person. Ett sådant beslut avser särskilt tillsynsmyndighetens utövande av utrednings-, korrigerings- och godkännandebefogenheter eller avvisande av eller avslag på klagomål. Denna rätt inbegriper dock inte tillsynsmyndigheters övriga åtgärder som inte är rättsligt bindande, såsom yttranden som avgetts eller rådgivning som tillhandahållits av tillsynsmyndigheten. Talan mot en tillsynsmyndighet bör väckas vid domstol i den medlemsstat där tillsynsmyndigheten är etablerad och bör prövas i enlighet med den nationella rätten i den medlemsstaten. Dessa domstolar bör ha fullständig behörighet, vilket bör omfatta behörighet att rättsligt eller faktiskt pröva alla frågor som rör de tvister som anhängiggjorts vid dem.

(87) Om en registrerad anser att hans eller hennes rättigheter enligt detta direktiv har kränkts bör han eller hon ha rätt att ge ett organ som syftar till att skydda registrerades rättigheter och intressen vad gäller skyddet av deras

personuppgifter, och som inrättats i enlighet med den nationella rätten i en medlemsstat, i uppdrag att på hans eller hennes vägnar lämna in ett klagomål till en tillsynsmyndighet och utöva rätten till rättsmedel. De registrerades rätt att bli företrädda bör inte påverka medlemsstatens nationella processrätt enligt vilken det kan vara obligatoriskt att registrerade företräds inför nationell domstol av en advokat enligt definitionen i rådets direktiv 77/249/EEG ([1]).

(88) Personer som lider skada till följd av behandling som står i strid med de bestämmelser som antas i enlighet med detta direktiv bör få ersättning av den personuppgiftsansvarige eller av någon annan myndighet som är behörig enligt medlemsstaternas nationella rätt. Begreppet *skada* bör tolkas brett mot bakgrund av domstolens rättspraxis och på ett sätt som fullt ut återspeglar detta direktivs mål. Detta påverkar inte skadeståndsanspråk till följd av överträdelser av andra bestämmelser i unionsrätten eller i medlemsstaternas nationella rätt. Vid hänvisning till behandling som är olaglig eller står i strid med de bestämmelser som antas i enlighet med detta direktiv omfattas även behandling som inte är i överensstämmelse med de genomförandeakter som antagits i enlighet med detta direktiv. Registrerade bör få full och effektiv ersättning för den skada de lidit.

(89) Om någon fysisk eller juridisk person överträder detta direktiv bör detta leda till sanktioner, oavsett om personen i fråga omfattas av privaträtt eller offentlig rätt. Medlemsstaterna bör säkerställa att sanktioner är effektiva, proportionella och avskräckande och bör vidta alla åtgärder som krävs för att sanktionerna ska verkställas.

(90) För att säkerställa enhetliga villkor för genomförandet av detta direktiv bör kommissionen tilldelas genomförandebefogenheter vad gäller adekvata skyddsnivåer i ett tredjeland, ett territorium eller en specificerad sektor inom ett tredjeland eller en internationell organisation och för format och förfaranden för ömsesidigt bistånd samt tillvägagångssätten för elektroniskt utbyte av information mellan tillsynsmyndigheter samt mellan tillsynsmyndigheter och styrelsen. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ([2]).

(91) Mot bakgrund av att dessa rättsakter har allmän räckvidd bör granskningsförfarandet användas vid antagandet av genomförandeakter om adekvata skyddsnivåer i ett tredjeland, ett territorium eller en specificerad sektor inom detta tredjeland eller en internationell organisation och om format och förfaranden för ömsesidigt bistånd samt tillvägagångssätten för elektroniskt utbyte av information mellan tillsynsmyndigheter samt mellan tillsynsmyndigheter och styrelsen.

(92) Kommissionen bör när tvingande skäl till skyndsamhet föreligger i vederbörligen motiverade fall anta omedelbart tillämpliga genomförandeakter avseende ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland eller en internationell organisation där en adekvat skyddsnivå inte längre kan säkerställas.

(93) Eftersom målen för detta direktiv, nämligen att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, och för att säkerställa ett fritt utbyte av personuppgifter mellan behöriga myndigheter inom 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 EU-fördraget. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå dessa mål.

(94) Särskilda bestämmelser i unionsakter på området för straffrättsligt samarbete och polissamarbete som antagits före dagen för antagandet av detta direktiv, och som reglerar behandlingen av personuppgifter mellan medlemsstaterna eller tillträdet för utsedda myndigheter i medlemsstaterna till informationssystem som inrättats i

([1]) Rådets direktiv 77/249/EEG av den 22 mars 1977 om underlättande för advokater att effektivt begagna sig av friheten att tillhandahålla tjänster (EGT L 78, 26.3.1977, s. 17).

([2]) 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).

enlighet med fördragen, bör kvarstå oförändrade, till exempel de särskilda bestämmelser om skydd av personuppgifter som tillämpas i enlighet med rådets beslut 2008/615/RIF ([1]), eller artikel 23 i konventionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater ([2]). Eftersom artikel 8 i stadgan och artikel 16 i EUF-fördraget kräver att den grundläggande rätten till skydd av personuppgifter bör säkerställas på ett enhetligt sätt i hela unionen bör kommissionen utvärdera situationen vad gäller förhållandet mellan detta direktiv och rättsakter, antagna före dagen för antagandet av detta direktiv, som reglerar behandling av personuppgifter mellan medlemsstaterna eller tillträde för utsedda myndigheter i medlemsstater till informationssystem som inrättats i enlighet med fördragen, i syfte att bedöma om dessa särskilda bestämmelser behöver anpassas till detta direktiv. Vid behov bör kommissionen lägga fram förslag i syfte att säkerställa enhetliga rättsregler angående behandlingen av personuppgifter.

(95) För att säkerställa ett övergripande och enhetligt skydd av personuppgifter i unionen bör internationella avtal som medlemsstaterna ingått före dagen för detta direktivs ikraftträdande, och som överensstämmer med relevant unionsrätt som var tillämplig före den dagen, fortsätta att gälla till dess att de ändras, ersätts eller upphävs.

(96) Medlemsstaterna bör medges en period på högst två år från dagen för ikraftträdandet av detta direktiv för att införliva det. Behandling som redan pågår den dagen bör bringas i överensstämmelse med detta direktiv inom en period av två år från det att detta direktiv träder i kraft. I fall där sådan behandling överensstämmer med unionsrätt som var tillämplig före dagen för ikraftträdandet av detta direktiv bör dock inte kraven i detta direktiv rörande förhandssamråd med tillsynsmyndigheten gälla för behandling som redan pågick vid den tidpunkten, eftersom dessa krav, p.g.a. sin natur, är sådana att de ska uppfyllas före själva behandlingen. Om medlemsstaterna tillämpar den längre genomförandeperioden som löper ut sju år efter detta direktivs ikraftträdande för fullgörandet av loggningsskyldigheterna för automatiserade behandlingssystem som inrättats före den dagen bör den personuppgiftsansvarige eller personuppgiftsbiträdet ha infört effektiva metoder, t.ex. loggar eller andra typer av register, för att visa att behandlingen av uppgifterna är laglig, möjliggöra egenkontroll samt säkerställa dataintegritet och datasäkerhet.

(97) Detta direktiv påverkar inte bestämmelserna om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi i Europaparlamentets och rådets direktiv 2011/93/EU ([3]).

(98) Rambeslut 2008/977/RIF bör därför upphävas.

(99) I enlighet med artikel 6a i protokoll nr 21 om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till EU-fördraget och EUF-fördraget, är Förenade kungariket och Irland inte bundna av de bestämmelser i detta direktiv som avser medlemsstaternas behandling av personuppgifter när de bedriver verksamhet som omfattas av avdelning V kapitel 4 eller 5 i tredje delen av EUF-fördraget i det fall då Förenade kungariket och Irland inte är bundna av bestämmelserna om formerna för straffrättsligt samarbete eller polissamarbete inom ramen för vilka de bestämmelser måste iakttas som fastställs på grundval av artikel 16 i EUF-fördraget.

(100) I enlighet med artiklarna 2 och 2a i protokoll nr 22 om Danmarks ställning, fogat till EU-fördraget och EUF-fördraget, är Danmark inte bundet av reglerna i detta direktiv och omfattas inte av den tillämpning av regler som avser medlemsstaternas behandling av personuppgifter när dessa utövar verksamhet som omfattas av tillämpningsområdet för kapitlen 4 och 5 i avdelning V i tredje delen i EUF-fördraget. Eftersom detta direktiv bygger på av Schengenregelverket, som omfattas av avdelning V i tredje delen av EUF-fördraget, ska Danmark i enlighet med artikel 4 i protokollet inom en tid av sex månader efter antagandet av detta direktiv besluta huruvida landet ska genomföra det i sin nationella lagstiftning.

(101) När det gäller Island och Norge utgör detta direktiv en vidareutveckling av bestämmelserna i Schengenregelverket i enlighet med avtalet mellan Europeiska unionens råd och Republiken Island och Konungariket Norge om dessa staters associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket ([4]).

([1]) Rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet (EUT L 210, 6.8.2008, s. 1).
([2]) Rådets akt av den 29 maj 2000 om att i enlighet med artikel 34 i Fördraget om Europeiska unionen upprätta konventionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater (EGT C 197, 12.7.2000, s. 1).
([3]) Europaparlamentets och rådets direktiv 2011/93/EU av den 13 december 2011 om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi samt om ersättande av rådets rambeslut 2004/68/RIF (EUT L 335, 17.12.2011, s. 1).
([4]) EGT L 176, 10.7.1999, s. 36.

(102) När det gäller Schweiz utgör detta direktiv, i enlighet med avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket, en utveckling av bestämmelserna i Schengenregelverket ([1]).

(103) När det gäller Liechtenstein utgör detta direktiv en vidareutveckling av bestämmelserna i Schengenregelverket i enlighet med protokollet mellan Europeiska unionen, Europeiska gemenskapen, Schweiziska edsförbundet och Furstendömet Liechtenstein om Furstendömet Liechtensteins anslutning till avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket ([2]).

(104) Detta direktiv respekterar de grundläggande rättigheterna och iakttar de principer som erkänns i stadgan som erkänns i EUF-fördraget, särskilt rätten till respekt för privatlivet och familjelivet, rätten till skydd av personuppgifter, rätt till ett effektivt rättsmedel och till en opartisk domstol. De inskränkningar som gjorts av dessa rättigheter överensstämmer med artikel 52.1 i stadgan eftersom de är nödvändiga för att uppnå av unionen erkända mål av allmänt intresse eller för att skydda andras rättigheter och friheter.

(105) I enlighet med den gemensamma politiska förklaringen av den 28 september 2011 från medlemsstaterna och kommissionen om förklarande dokument, har medlemsstaterna åtagit sig att, i de fall detta är berättigat, låta anmälan av införlivandeåtgärder åtföljas av ett eller flera dokument som förklarar förhållandet mellan de olika delarna i direktivet och motsvarande delar i de nationella införlivandeåtgärderna. Med avseende på detta direktiv anser lagstiftaren att översändandet av sådana dokument är berättigat.

(106) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i Europaparlamentets och rådets förordning (EG) nr 45/2001 och avgav ett yttrande den 7 mars 2012 ([3]).

(107) Detta direktiv bör inte hindra medlemsstaterna från att i nationell straffprocesslagstiftning genomföra bestämmelser om registrerades utövande av sina rättigheter vad gäller information, tillgång till och rättelse eller radering av personuppgifter och begränsning av behandling i samband med straffrättsliga förfaranden samt eventuella begränsningar av dessa rättigheter.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Allmänna bestämmelser

Artikel 1

Syfte och mål

1. I detta direktiv fastställs bestämmelser om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av behöriga myndigheter 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.

2. Enligt detta direktiv ska medlemsstaterna

a) skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, och

b) säkerställa att behöriga myndigheters utbyte av personuppgifter inom unionen, när sådant utbyte krävs enligt unionsrätten eller medlemsstaternas nationella rätt, varken begränsas eller förbjuds av skäl som rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter.

([1]) EUT L 53, 27.2.2008, s. 52.
([2]) EUT L 160, 18.6.2011, s. 21.
([3]) EGT C 192, 30.6.2012, s. 7.

3. Detta direktiv ska inte hindra medlemsstaterna från att föreskriva starkare skyddsåtgärder än de som fastställs i detta direktiv för skyddet av den registrerades rättigheter och friheter med avseende på behöriga myndigheters behandling av personuppgifter.

Artikel 2

Tillämpningsområde

1. Detta direktiv ska tillämpas på behandling av personuppgifter som utförs av behöriga myndigheter för de ändamål som anges i artikel 1.1.

2. Detta direktiv ska tillämpas på behandling av personuppgifter som helt eller delvis företas på automatiserad väg samt på annan behandling än automatiserad behandling av personuppgifter som ingår i eller kommer att ingå i ett register.

3. Detta direktiv tillämpas inte på behandling av personuppgifter

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

b) som utförs av unionens institutioner, organ och byråer.

Artikel 3

Definitioner

I detta direktiv avses med

1. *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar enskild person (nedan kallad *en registrerad*), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras, särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer, eller till 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 automatiserad 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 aspekter rörande 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. *behörig myndighet*:

   a) en offentlig myndighet som har behörighet att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga hot mot den allmänna säkerheten, eller

   b) annat organ eller annan enhet som genom medlemsstaternas nationella rätt har anförtrotts myndighetsutövning för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten,

8. *personuppgiftsansvarig*: en behörig myndighet som ensam 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 föreskrivs i unionsrätten eller medlemsstaternas nationella rätt,

9. *personuppgiftsbiträde*: en fysisk eller juridisk person, myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,

10. *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,

11. *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,

12. *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,

13. *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 unik identifiering av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter,

14. *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,

15. *tillsynsmyndighet*: en oberoende offentlig myndighet som är utsedd av en medlemsstat i enlighet med artikel 41,

16. *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 4

Principer för behandling av personuppgifter

1. Medlemsstaterna ska föreskriva att personuppgifter ska

a) behandlas på ett lagligt och korrekt sätt,

b) samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte behandlas på ett sätt som står i strid med dessa ändamål,

c) vara adekvata, relevanta och inte för omfattande i förhållande till de syften för vilka de behandlas,

d) 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,

e) 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 de behandlas,

f) 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.

2. Behandling som utförs av samma eller en annan personuppgiftsansvarig för något annat ändamål som anges i artikel 1.1 än det för vilket personuppgifterna samlas in ska tillåtas om

a) den personuppgiftsansvarige i enlighet med unionsrätten eller medlemsstaternas nationella rätt är bemyndigad att behandla sådana personuppgifter för ett sådant ändamål, och

b) behandlingen är nödvändig och står i proportion till detta andra ändamål i enlighet med unionsrätten eller medlemsstaternas nationella rätt.

3. Behandling som utförs av samma eller en annan personuppgiftsansvarig kan inbegripa arkivändamål av allmänt intresse och vetenskaplig, statistisk eller historisk användning för de ändamål som anges i artikel 1.1 under förutsättning att det finns lämpliga skyddsåtgärder för de registrerades rättigheter och friheter.

4. Den personuppgiftsansvarige ska ansvara för, och kunna visa efterlevnad av, punkterna 1, 2 och 3.

Artikel 5

Tidsgränser för lagring och översyn

Medlemsstaterna ska föreskriva att lämpliga tidsgränser fastställs för radering av personuppgifter eller för periodisk översyn av behovet av att lagra personuppgifter. Procedurrelaterade åtgärder ska säkerställa att tidsgränserna efterlevs.

Artikel 6

Åtskillnad mellan olika kategorier av registrerade

Medlemsstaterna ska föreskriva att den personuppgiftsansvarige, i tillämpliga fall och så långt det är möjligt, ska göra en klar åtskillnad mellan personuppgifter som rör olika kategorier av registrerade, såsom

a) personer avseende vilka det finns tungt vägande skäl att anta att de har begått eller är på väg att begå ett brott,

b) personer som dömts för brott,

c) brottsoffer eller personer avseende vilka det finns vissa omständigheter som ger anledning att anta att de kan vara brottsoffer, och

d) andra som berörs av ett brott, såsom personer som kan komma att kallas att vittna i samband med brottsutredningar eller senare straffrättsliga förfaranden, personer som kan ge information om brott eller personer med kontakter med eller band till någon av de personer som avses i a och b.

Artikel 7

Åtskillnad mellan personuppgifter och kontroll av kvaliteten på personuppgifterna

1. Medlemsstaterna ska föreskriva att personuppgifter som grundar sig på fakta så långt det är möjligt ska åtskiljas från personuppgifter som grundar sig på personliga bedömningar.

2. Medlemsstaterna ska föreskriva att de behöriga myndigheterna ska vidta alla rimliga åtgärder för att se till att personuppgifter som är felaktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga. Varje behörig myndighet ska därför i den mån det är praktiskt möjligt kontrollera kvaliteten på personuppgifterna innan dessa överförs eller görs tillgängliga. Vid all överföring av personuppgifter ska, så långt det är möjligt, sådan nödvändig information läggas till som gör det möjligt för den mottagande behöriga myndigheten att bedöma i vilken grad personuppgifterna är korrekta, fullständiga och tillförlitliga samt i vilken utsträckning de är aktuella.

3. Om det visar sig att felaktiga personuppgifter har överförts eller att personuppgifter olagligen har överförts ska mottagaren omedelbart underrättas om detta. I sådana fall ska personuppgifterna rättas eller raderas eller behandlingen begränsas i enlighet med artikel 16.

Artikel 8

Laglig behandling av personuppgifter

1. Medlemsstaterna ska föreskriva att behandling ska vara laglig endast om och i den mån behandlingen är nödvändig för att utföra en uppgift som utförs av en behörig myndighet för de ändamål som anges i artikel 1.1 och som sker på grundval av unionsrätt eller medlemsstaternas nationella rätt.

2. Medlemsstaternas nationella rätt som reglerar behandling inom tillämpningsområdet för detta direktiv ska åtminstone specificera syftet med behandlingen, vilka personuppgifter som ska behandlas och behandlingens ändamål.

Artikel 9

Särskilda villkor för uppgiftsbehandling

1. Personuppgifter som samlas in av behöriga myndigheter för de ändamål som anges i artikel 1.1. ska inte behandlas för andra ändamål än de som anges i artikel 1.1 såvida inte sådan behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt. När personuppgifter behandlas för andra ändamål ska förordning (EU) 2016/679 tillämpas, såvida inte behandlingen utförs som ett led i en verksamhet som inte omfattas av unionsrätten.

2. Om de behöriga myndigheterna enligt medlemsstaternas nationella rätt anförtros utförandet av andra uppgifter än de som utförs för de ändamål som anges i artikel 1.1, ska förordning (EU) 2016/679 vara tillämplig på behandlingen för dessa ändamål, inklusive för arkivändamål av allmänt intresse, för historiska eller vetenskapliga forskningsändamål eller för statistiska ändamål, såvida inte behandlingen utförs som ett led i en verksamhet som inte omfattas av unionsrätten.

3. Om den unionsrätt eller nationella rätt som är tillämplig på den överförande behöriga myndigheten fastställer särskilda villkor för behandling, ska medlemsstaten föreskriva att den överförande behöriga myndigheten ska informera mottagaren om dessa särskilda villkor och om kravet att respektera dem.

4. Medlemsstaterna ska föreskriva att den överförande behöriga myndigheten inte ska tillämpa villkor enligt punkt 3 på mottagare i andra medlemsstater eller på byråer och organ som inrättats i enlighet med avdelning V kapitlen 4 och 5 i EUF-fördraget, med undantag för de villkor som är tillämpliga på motsvarande överföringar av uppgifter inom den överförande behöriga myndighetens medlemsstat.

Artikel 10

Behandling av särskilda kategorier av personuppgifter

Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, samt behandling av genetiska uppgifter, biometriska uppgifter för att unikt identifiera en fysisk person eller uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning ska vara tillåten endast om det är absolut nödvändigt och under förutsättning att det finns lämpliga skyddsåtgärder för den registrerades rättigheter och friheter och endast

a) om behandlingen är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt,

b) för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan fysisk person, eller

c) om behandlingen rör uppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.

Artikel 11

Automatiserat individuellt beslutsfattande

1. Medlemsstaterna ska föreskriva att beslut som enbart grundas på automatiserad behandling, inbegripet profilering, som har negativa rättsliga följder för den registrerade eller i betydande grad påverkar honom eller henne, ska förbjudas om de inte är tillåtna enligt unionsrätten eller medlemsstaternas nationella rätt som den personuppgiftsansvarige lyder under och som föreskriver lämpliga skyddsåtgärder för den registrerades rättigheter och friheter, åtminstone rätten till mänskligt ingripande från den personuppgiftsansvariges sida.

2. Beslut som avses i punkt 1 i den här artikeln får inte grundas på de särskilda kategorier av personuppgifter som avses i artikel 10, såvida inte lämpliga åtgärder för att skydda den registrerades rättigheter och friheter samt berättigade intressen har vidtagits.

3. Profilering som leder till diskriminering av fysiska personer på grundval av särskilda kategorier av personuppgifter enligt artikel 10 ska förbjudas i enlighet med unionsrätten.

KAPITEL III

Den registrerades rättigheter

Artikel 12

Information om och villkor för utövandet av den registrerades rättigheter

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska vidta rimliga åtgärder för att tillhandahålla den registrerade all information som avses i artikel 13 och alla meddelanden enligt artiklarna 11, 14–18 och 31 som avser behandling i en koncis, begriplig och lättillgänglig form och på ett klart och tydligt språk. Informationen ska tillhandahållas på lämpligt sätt, t.ex. elektroniskt. Som en allmän regel ska den personuppgiftsansvarige tillhandahålla informationen i samma format som begäran.

2. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska underlätta utövandet av den registrerades rättigheter enligt artiklarna 11 och 14–18.

3. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige utan onödigt dröjsmål skriftligen ska informera den registrerade om uppföljningen av hans eller hennes begäran.

4. Medlemsstaterna ska föreskriva att den information som tillhandahålls enligt artikel 13 och alla meddelanden eller åtgärder som vidtas enligt artiklarna 11, 14–18 och 31 ska tillhandahållas kostnadsfritt. Om en registrerads begäran är uppenbart ogrundad eller orimlig, särskilt på grund av att den är repetitiv, får den personuppgiftsansvarige antingen

a) ta ut en rimlig avgift med beaktande av de administrativa kostnaderna för tillhandahållandet av informationen eller meddelandet eller vidtagandet av den åtgärd som begärs, eller

b) vägra att tillmötesgå begäran.

Den personuppgiftsansvarige ska visa att begäran är uppenbart ogrundad eller orimlig.

5. Om den personuppgiftsansvarige har rimliga skäl att betvivla identiteten hos den fysiska person som lämnar in en begäran enligt artiklarna 14 eller 16, får den personuppgiftsansvarige begära att ytterligare information som är nödvändig för att bekräfta den registrerades identitet ska tillhandahållas.

Artikel 13

Information som ska göras tillgänglig för eller lämnas till den registrerade

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska göra åtminstone följande information tillgänglig för den registrerade:

a) Den personuppgiftsansvariges identitet och kontaktuppgifter.

b) Dataskyddsombudets kontaktuppgifter, i tillämpliga fall.

c) Ändamålen med den behandling för vilken personuppgifterna är avsedda.

d) Rätten att lämna in klagomål till en tillsynsmyndighet samt tillsynsmyndighetens kontaktuppgifter.

e) Rätten att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter och begränsning av behandlingen av personuppgifter som rör den registrerade.

2. Utöver den information som avses i punkt 1, ska medlemsstaterna i lag föreskriva att den personuppgiftsansvarige i specifika fall ska lämna följande information till den registrerade, för att göra det möjligt för honom eller henne att utöva sina rättigheter:

a) Behandlingens rättsliga grund.

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

c) I tillämpliga fall, kategorierna av mottagare av personuppgifterna, inbegripet i tredjeländer eller internationella organisationer.

d) Vid behov ytterligare information, i synnerhet om personuppgifterna samlas in utan den registrerades vetskap.

3. Medlemsstaterna får anta lagstiftningsåtgärder som gör att informationen till den registrerade enligt punkt 2 senareläggs, begränsas eller utelämnas, i den utsträckning och så länge som en sådan åtgärd är nödvändig och proportionell i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, i syfte att

a) undvika att hindra officiella eller rättsliga utredningar, undersökningar eller förfaranden,

b) undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder,

c) skydda den allmänna säkerheten,

d) skydda den nationella säkerheten,

e) skydda andra personers rättigheter och friheter.

4. Medlemsstaterna får anta lagstiftningsåtgärder för att fastställa kategorier av behandling som helt eller delvis kan omfattas av något av leden i punkt 3.

Artikel 14

Den registrerades rätt till tillgång till personuppgifter

Med förbehåll för artikel 15 ska medlemsstaterna föreskriva att den registrerade ska ha rätt att av den personuppgiftsansvarige få bekräftelse av 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 och dess rättsliga grund.

b) De kategorier av personuppgifter som behandlingen gäller.

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

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

e) Rätten att av den personuppgiftsansvarige begära rättelse eller radering av personuppgifter eller begränsning av behandling av personuppgifter som rör den registrerade.

f) Rätten att lämna in klagomål till tillsynsmyndigheten samt tillsynsmyndighetens kontaktuppgifter.

g) Information om vilka personuppgifter som håller på att behandlas och all tillgänglig information om varifrån dessa uppgifter härstammar.

Artikel 15

Begränsningar av rätten till tillgång

1. Medlemsstaterna får anta lagstiftningsåtgärder som helt eller delvis begränsar den registrerades rätt till tillgång i den utsträckning och så länge en sådan partiell eller fullständig begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, i syfte att

a) undvika att hindra officiella eller rättsliga utredningar, förundersökningar eller förfaranden,

b) undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder,

c) skydda den allmänna säkerheten,

d) skydda den nationella säkerheten,

e) skydda andra personers rättigheter och friheter.

2. Medlemsstaterna får anta lagstiftningsåtgärder för att fastställa kategorier av behandling som helt eller delvis kan omfattas av undantagen i punkt 1 a–e.

3. I de fall som avses i punkterna 1 och 2 ska medlemsstaterna föreskriva att den personuppgiftsansvarige utan onödigt dröjsmål ska informera den registrerade skriftligen om varje vägran eller begränsning av tillgång och om skälen för vägran eller begränsningen. Denna information kan utelämnas om tillhandahållandet skulle undergräva ett ändamål enligt punkt 1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska underrätta den registrerade om möjligheten att lämna in ett klagomål till en tillsynsmyndighet eller begära rättslig prövning.

4. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska dokumentera de sakliga och rättsliga grunderna för beslutet. Denna information ska göras tillgänglig för tillsynsmyndigheterna.

Artikel 16

Rätt till rättelse eller radering av personuppgifter och begränsning av behandling

1. Medlemsstaterna ska föreskriva att den registrerade ska ha rätt att utan onödigt dröjsmål av den personuppgiftsansvarige få felaktiga personuppgifter som rör honom eller henne rättade. Med beaktande av ändamålet med behandlingen ska medlemsstaterna föreskriva att den registrerade ska ha rätt att få ofullständiga personuppgifter kompletterade, inbegripet genom att tillhandahålla en kompletterande inlaga.

2. Medlemsstaterna ska kräva att den personuppgiftsansvarige utan onödigt dröjsmål ska radera personuppgifter och ge den registrerade rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få till stånd radering av personuppgifter som rör honom eller henne om behandlingen står i strid med de bestämmelser som antas enligt artiklarna 4, 8 och 10 eller om personuppgifterna måste raderas för att uppfylla en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

3. I stället för radering ska den personuppgiftsansvarige begränsa behandling om

a) den registrerade bestrider personuppgifternas korrekthet och korrektheten inte kan fastställas, eller

b) personuppgifterna måste sparas som bevisning.

Om behandlingen begränsas enligt första stycket led a ska den personuppgiftsansvarige underrätta den registrerade innan begränsningen av behandlingen upphävs.

4. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige underrättar den registrerade skriftligen om eventuell vägran att rätta, radera eller begränsa behandlingen och om skälen till vägran. Medlemsstaterna får anta lagstiftningsåtgärder som helt eller delvis begränsar skyldigheten att tillhandahålla sådan information i den utsträckning som en sådan begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, i syfte att

a) undvika att hindra offentliga eller rättsliga utredningar, undersökningar eller förfaranden,

b) undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder,

c) skydda den allmänna säkerheten,

d) skydda den nationella säkerheten,

e) skydda andra personers rättigheter och friheter.

Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska underrätta den registrerade om möjligheterna att lämna in ett klagomål till en tillsynsmyndighet eller begära rättslig prövning.

5. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska meddela varje rättelse av oriktiga personuppgifter till den behöriga myndighet från vilken de oriktiga personuppgifterna kommer.

6. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige, när personuppgifter har rättats, raderats eller begränsats i enlighet med punkterna 1, 2 och 3, ska underrätta mottagarna och att mottagarna ska rätta eller radera personuppgifterna eller begränsa den behandling som utförs under deras ansvar.

Artikel 17

Den registrerades utövande av rättigheter och kontroll genom tillsynsmyndigheten

1. I de fall som avses i artiklarna 13.3, 15.3 och 16.4 ska medlemsstaterna anta bestämmelser om att den registrerades rättigheter även kan utövas genom den behöriga tillsynsmyndigheten.

2. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska underrätta den registrerade om hans eller hennes möjlighet att utöva sina rättigheter genom tillsynsmyndigheten enligt punkt 1.

3. När den rättighet som avses i punkt 1 utövas ska tillsynsmyndigheten åtminstone underrätta den registrerade om att alla nödvändiga kontroller eller en översyn genom tillsynsmyndigheten har ägt rum. Tillsynsmyndigheten ska också informera den registrerade om hans eller hennes rätt att begära rättslig prövning.

Artikel 18

Den registrerades rättigheter i brottsutredningar och straffrättsliga förfaranden

Medlemsstaterna får föreskriva att de rättigheter som avses i artiklarna 13, 14 och 16 ska utövas i enlighet med medlemsstaternas nationella rätt om personuppgifterna ingår i ett domstolsbeslut eller ett rättsligt protokoll eller ärende som behandlas i samband med brottsutredningar och straffrättsliga förfaranden.

KAPITEL IV

Personuppgiftsansvarig och personuppgiftsbiträde

Avsnitt 1

Allmänna skyldigheter

Artikel 19

Den personuppgiftsansvariges skyldigheter

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige, med beaktande av behandlingens art, omfattning, sammanhang och ändamål, samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter, ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa, och kunna visa, att behandlingen utförs i enlighet med detta direktiv. 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.

Artikel 20

Inbyggt dataskydd och dataskydd som standard

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige, med beaktande av den senaste utvecklingen och genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål, samt de risker, av varierande sannolikhetsgrad och allvar för fysiska personers rättigheter och friheter som behandlingen utgör, både vid tidpunkten för beslut om vilka medel behandlingen ska utföras med och vid tidpunkten för själva behandlingen, ska genomföra lämpliga tekniska och organisatoriska åtgärder, såsom pseudonymisering, vilka är utformade för genomförande av dataskyddsprinciper, såsom uppgiftsminimering, på ett effektivt sätt och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, för att uppfylla kraven i detta direktiv och skydda den registrerades rättigheter.

2. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige genomför 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.

Artikel 21

Gemensamt personuppgiftsansvariga

1. Medlemsstaterna ska föreskriva att två eller flera personuppgiftsansvariga har gemensamt ansvar för registret, om de gemensamt fastställer behandlingens ändamål och medel. De ska under öppna former fastställa sitt respektive ansvar för efterlevnaden av detta direktiv, särskilt vad gäller utövandet av den registrerades rättigheter och sina respektive skyldigheter att tillhandahålla den information som avses i artikel 13, genom ett inbördes arrangemang, såvida inte och i den mån som de personuppgiftsansvarigas respektive skyldigheter fastställs i unionsrätt eller medlemsstaternas nationella rätt som de personuppgiftsansvariga omfattas av. Inom ramen för arrangemanget ska en kontaktpunkt för de registrerade utses. Medlemsstaterna får fastslå vem av de gemensamt personuppgiftsansvariga som kan fungera som enda kontaktpunkt för de registrerade i fråga om utövandet av deras rättigheter.

2. Oavsett formerna för det arrangemang som avses i punkt 1 får medlemsstaterna föreskriva att den registrerade får utöva sina rättigheter enligt de bestämmelser som antas i enlighet med detta direktiv med avseende på var och en av de personuppgiftsansvariga.

Artikel 22

Personuppgiftsbiträde

1. Medlemsstaterna ska, om en behandling ska genomföras på en personuppgiftsansvarigs vägnar, föreskriva att den personuppgiftsansvarige endast ska anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i detta direktiv och säkerställer att den registrerades rättigheter skyddas.

2. Medlemsstaterna ska föreskriva att personuppgiftsbiträdet inte får 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 alltid 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. Medlemsstaterna ska föreskriva att ett personuppgiftsbiträdes behandling ska regleras genom ett avtal eller annan rättsakt enligt unionsrätten eller 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. Avtalet eller den andra rättsakten ska särskilt föreskriva att personuppgiftsbiträdet

a) endast handlar enligt instruktioner från den personuppgiftsansvarige,

b) säkerställer att personer som har tillstånd att behandla personuppgifterna har förbundit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt,

c) på lämpligt sätt ska bistå den personuppgiftsansvarige att säkerställa efterlevnad av bestämmelserna om den registrerades rättigheter,

d) beroende på vad den personuppgiftsansvarige väljer, ska radera eller återlämna alla personuppgifter till den personuppgiftsansvarige efter det att tillhandahållandet av uppgiftsbehandlingstjänster har avslutats och raderar befintliga kopior, såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt,

e) ska ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att denna artikel efterlevs,

f) respekterar de villkor som avses i punkterna 2 och 3 för anlitande av ett annat personuppgiftsbiträde.

4. Det avtal eller den andra rättsakt som avses i punkt 3 ska vara skriftligt, inbegripet i elektronisk form.

5. Om ett personuppgiftsbiträde i strid med detta direktiv fastställer ändamålen och medlen för behandlingen ska personuppgiftsbiträdet anses vara personuppgiftsansvarig med avseende på den behandlingen.

Artikel 23

Behandling under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende

Medlemsstaterna ska föreskriva att personuppgiftsbiträdet och personer som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, endast får behandla dessa uppgifter enligt instruktion från den personuppgiftsansvarige, såvida han eller hon inte är skyldig att göra det enligt unionsrätten eller medlemsstaternas nationella rätt.

Artikel 24

Register över behandling

1. Medlemsstaterna ska föreskriva att alla personuppgiftsansvariga ska föra ett register över alla kategorier av verksamheter i samband med behandling som de ansvarar för. Detta register ska innehålla samtliga följande uppgifter:

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

b) Ändamålen med behandlingen.

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

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

e) Användning av profilering, i tillämpliga fall.

f) I tillämpliga fall, kategorier av personuppgiftsöverföringar till ett tredjeland eller en internationell organisation.

g) En uppgift om den rättsliga grunden för den behandling, inbegripet överföringar, för vilken personuppgifterna är avsedda.

h) Om möjligt, de planerade tidsfristerna för radering av de olika personuppgiftskategorierna.

i) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 29.1.

2. Medlemsstaterna ska föreskriva att alla personuppgiftsbiträden ska upprätthålla ett register över alla kategorier av behandling som utförts för den personuppgiftsansvariges räkning, vilket ska omfatta följande:

a) Namn och kontaktuppgifter för personuppgiftsbiträdet eller registerförarna, för varje personuppgiftsansvarig för vars räkning personuppgiftsbiträdet agerar samt, i tillämpliga fall, för dataskyddsombudet.

b) De kategorier av behandling som har utförts för varje personuppgiftsansvarigs räkning.

c) I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen, om den personuppgiftsansvarige uttryckligen begär detta.

d) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 29.1.

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

Den personuppgiftsansvarige och personuppgiftsbiträdet ska på begäran göra registren tillgängliga för tillsynsmyndigheten.

Artikel 25

Loggning

1. Medlemsstaterna ska säkerställa att loggar förs över åtminstone följande typer av behandlingar i automatiserade behandlingssystem: insamling, ändring, läsning, utlämning inbegripet överföringar, sammanförande och radering. Loggarna över läsning och utlämning ska göra det möjligt att fastställa motivering, datum och tidpunkt för sådan behandling och i möjligaste mån vem som har läst eller lämnat ut personuppgifter, samt vilka som har fått tillgång till personuppgifterna.

2. Loggarna bör endast användas för att kontrollera om behandlingen är tillåten, för egenkontroll, för att säkerställa personuppgifternas integritet och säkerhet, samt inom ramen för straffrättsliga förfaranden.

3. Den personuppgiftsansvarige och personuppgiftsbiträdet ska på begäran göra loggarna tillgängliga för tillsynsmyndigheten.

Artikel 26

Samarbete med tillsynsmyndigheten

Medlemsstaterna ska föreskriva att den personuppgiftsansvarige och personuppgiftsbiträdet på begäran ska samarbeta med tillsynsmyndigheten vid utförandet av dess uppgifter.

Artikel 27

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 medlemsstaterna säkerställa att den personuppgiftsansvarige före behandlingen utför en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter.

2. Den bedömning som avses i punkt 1 ska åtminstone innehålla en allmän beskrivning av den planerade behandlingen, en bedömning av riskerna för de registrerades rättigheter och friheter, de åtgärder som planeras för att hantera dessa risker, skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifter och för att visa att detta direktiv efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.

Artikel 28

Förhandssamråd med tillsynsmyndigheten

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige eller personuppgiftsbiträdet ska samråda med tillsynsmyndigheten före behandling av personuppgifter som kommer att ingå i ett nytt register som ska inrättas, om

a) en konsekvensbedömning avseende dataskydd enligt artikel 27 visar att behandlingen skulle leda till en hög risk om inte den registeransvarige vidtar åtgärder för att minska risken, eller om

b) typen av behandling, särskilt vid användning av ny teknik eller nya rutiner eller förfaranden, medför en hög risk för de registrerades rättigheter och friheter.

2. Medlemsstaterna ska föreskriva att tillsynsmyndigheten ska rådfrågas under 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.

3. Medlemsstaterna ska föreskriva att tillsynsmyndigheten får upprätta en förteckning över de olika typer av uppgiftsbehandling som omfattas av förhandssamråd enligt punkt 1.

4. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige till tillsynsmyndigheten lämnar in den konsekvensbedömning avseende dataskydd som avses i artikel 27 och, på begäran, eventuell övrig information som gör att tillsynsmyndigheten kan göra en bedömning av behandlingens överensstämmelse och särskilt av riskerna för skyddet av den registrerades personuppgifter och av därmed sammanhängande skyddsåtgärder.

5. Medlemsstaterna ska, om tillsynsmyndigheten anser att den planerade behandling som avses i punkt 1 i denna artikel inte skulle vara förenlig med de bestämmelser som antas i enlighet med detta direktiv, särskilt om den personuppgiftsansvarige inte i tillräcklig mån har fastställt eller reducerat risken, föreskriva att tillsynsmyndigheten inom en period på högst sex veckor från det att begäran om samråd mottagits ska ge den personuppgiftsansvarige och, i tillämpliga fall, personuppgiftsbiträdet skriftliga råd och får utnyttja alla de befogenheter som den har enligt artikel 47. Denna period får förlängas med en månad 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.

Avsnitt 2

Säkerhet för personuppgifter

Artikel 29

Säkerhet i samband med behandling

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige och personuppgiftsbiträdet, med beaktande av den senaste utvecklingen och genomförandekostnader och med hänsyn till behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter, ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, i synnerhet när det gäller de särskilda kategorier av personuppgifter som avses i artikel 10.

2. När det gäller automatiserad behandling ska varje medlemsstat föreskriva att den personuppgiftsansvarige eller personuppgiftsbiträdet, efter en bedömning av riskerna, ska vidta åtgärder i syfte att

a) vägra varje obehörig person åtkomst till utrustning för behandling som används för behandling (*åtkomstskydd för utrustning*),

b) förhindra obehörig läsning, kopiering, ändring eller radering av datamedier (*kontroll av datamedier*),

c) förhindra obehörig registrering av personuppgifter och obehörig kännedom om, ändring eller radering av lagrade personuppgifter (*lagringskontroll*),

d) förhindra att obehöriga kan använda automatiserade behandlingssystem med hjälp av utrustning för dataöverföring (*användarkontroll*),

e) säkerställa att personer som är behöriga att använda ett automatiserat behandlingssystem endast har tillgång till personuppgifter som omfattas av deras behörighet (*åtkomstkontroll*),

f) säkerställa att det kan kontrolleras och fastställas till vilka organ personuppgifter har överförts eller kan överföras och för vilka organ uppgifterna har gjorts tillgängliga eller kan göras tillgängliga med hjälp av utrustning för dataöverföring (*kommunikationskontroll*),

g) säkerställa att det är möjligt att i efterhand kontrollera och fastställa vilka personuppgifter som förts in i ett automatiserat behandlingssystem, samt när och av vem personuppgifterna infördes (*indatakontroll*),

h) förhindra obehörig läsning, kopiering, ändring eller radering av personuppgifter i samband med överföring av sådana uppgifter eller under transport av databärare (*transportkontroll*),

i) säkerställa att de system som används kan återställas vid störningar (*återställande*),

j) säkerställa att systemet fungerar, att funktionsfel rapporteras (*driftsäkerhet*) och att de lagrade personuppgifterna inte kan förvanskas genom funktionsfel i systemet (*dataintegritet*).

Artikel 30

Anmälan av en personuppgiftsincident till tillsynsmyndigheten

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige vid en personuppgiftsincident utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om incidenten, anmäler den till tillsynsmyndigheten, 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 antal registrerade som berörs samt de kategorier av och det ungefärliga antal personuppgiftsposter som berörs,

b) förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller annan kontaktpunkt där mer information kan erhållas,

c) beskriva de sannolika konsekvenserna av personuppgiftsincidenten,

d) beskriva de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, i tillämpliga fall, 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. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter som avses i punkt 1, inbegripet omständigheterna rörande personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av denna artikel.

6. Medlemsstaterna ska föreskriva att den information som avses i punkt 3, om personuppgiftsincidenten rör personuppgifter som har överförts av eller till den personuppgiftsansvarige i en annan medlemsstat, utan onödigt dröjsmål ska meddelas den personuppgiftsansvarige i den medlemsstaten.

Artikel 31

Information till den registrerade om en personuppgiftsincident

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige, om personuppgiftsincidenten sannolikt kommer att leda till en hög risk för fysiska personers rättigheter och friheter, utan onödigt dröjsmål ska informera den registrerade om personuppgiftsincidenten.

2. Den information till den registrerade som avses i punkt 1 i den här artikeln ska innehålla en tydlig och klar beskrivning av personuppgiftsincidentens art och åtminstone de upplysningar och åtgärder som avses i artikel 30.3 b, c och d.

3. Information till den registrerade i enlighet med punkt 1 ska inte krävas om något av följande villkor är uppfyllda:

a) Den personuppgiftsansvarige har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder och dessa åtgärder har tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten, i synnerhet sådana som gör personuppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till dem, såsom kryptering.

b) Om 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 personuppgiftsbiträdet 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 besluta att något av de villkor som avses i punkt 3 är uppfyllt.

5. Den information till den registrerade som avses i punkt 1 i den här artikeln kan senareläggas, begränsas eller utelämnas på de villkor och av de skäl som avses i artikel 13.3.

Avsnitt 3

Dataskyddsombud

Artikel 32

Utnämning av dataskyddsombudet

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska utnämna ett dataskyddsombud. Medlemsstaterna får undanta domstolars och andra oberoende rättsliga myndigheters dömande verksamhet från denna skyldighet.

2. Dataskyddsombudet ska utnämnas på grundval av sina yrkesmässiga kvalifikationer och, i synnerhet, sin sakkunskap om lagstiftning och praxis i fråga om dataskydd samt förmåga att fullgöra de uppgifter som avses i artikel 34.

3. Ett enda dataskyddsombud får utnämnas för flera behöriga myndigheter med hänsyn tagen till organisationsstruktur och storlek.

4. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till tillsynsmyndigheten.

Artikel 33

Dataskyddsombudets ställning

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.

2. Den personuppgiftsansvarige ska stödja dataskyddsombudet i utförandet av de uppgifter som avses i artikel 34 genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter samt tillgång till personuppgifter och behandlingsförfaranden, samt i upprätthållandet av dennes sakkunskap.

Artikel 34

Dataskyddsombudets uppgifter

Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska anförtro dataskyddsombudet åtminstone följande uppgifter:

a) Att informera och ge råd till den personuppgiftsansvarige och de anställda som utför behandling om deras skyldigheter enligt detta direktiv och annan unionsrätt eller medlemsstaters bestämmelser om dataskydd.

b) Att övervaka efterlevnaden av detta direktiv, annan unionsrätt eller medlemsstaternas bestämmelser om dataskydd och av den personuppgiftsansvariges strategier för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandlingen och tillhörande granskning.

c) Att på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den enligt artikel 27.

d) Att samarbeta med tillsynsmyndigheten.

e) Att fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling, inbegripet det förhandssamråd som avses i artikel 28, och, om så är lämpligt, samråda i andra frågor.

KAPITEL V

Överföringar av personuppgifter till tredjeländer eller internationella organisationer

Artikel 35

Allmänna principer för överföringar av personuppgifter

1. Medlemsstaterna ska föreskriva att de behöriga myndigheterna endast ska överföra personuppgifter som håller på att behandlas eller är avsedda att behandlas efter det att de överförts till ett tredjeland eller en internationell organisation, inklusive för vidare överföring till ett annat tredjeland eller en annan internationell organisation, under förutsättning att de nationella bestämmelser som antas i enlighet med andra bestämmelser i detta direktiv respekteras och endast om de villkor som fastställs i detta kapitel uppfylls, nämligen:

a) Överföringen är nödvändig för de ändamål som anges i artikel 1.1.

b) Personuppgifterna överförs till en personuppgiftsansvarig i ett tredjeland eller en internationell organisation som är en behörig myndighet för de ändamål som avses i artikel 1.1.

c) Den aktuella medlemsstaten, om personuppgifter överförs eller görs tillgängliga från en annan medlemsstat, har gett förhandstillstånd till överföringen i enlighet med medlemsstaternas nationella rätt.

d) Kommissionen har antagit ett beslut om adekvat skyddsnivå i enlighet med artikel 36 eller, om inget sådant beslut föreligger, när lämpliga skyddsåtgärder har vidtagits eller föreligger enligt artikel 37 eller, om inget beslut om adekvat skyddsnivå enligt artikel 36 föreligger och inga lämpliga skyddsåtgärder enligt artikel 37 har vidtagits, när undantag för särskilda situationer gäller i enlighet med artikel 38.

e) Att den behöriga myndighet som gjorde den ursprungliga överföringen eller en annan behörig myndighet i samma medlemsstat vid vidare överföring till ett annat tredjeland eller en internationell organisation godkänner vidareöverföringen efter vederbörligt beaktande av alla relevanta faktorer, inbegripet brottets allvar, det ändamål för vilket personuppgifterna ursprungligen överfördes och nivån på skyddet av personuppgifter i tredjelandet till vilket eller den internationella organisationen till vilken personuppgifterna förts vidare.

2. Medlemsstaterna ska föreskriva att överföringar utan förhandstillstånd av en annan medlemsstat i enlighet med punkt 1 c tillåts endast om överföringen av personuppgifter är nödvändig för att avvärja ett omedelbart och allvarligt hot mot den allmänna säkerheten i en medlemsstat eller ett tredjeland eller mot en medlemsstats väsentliga intressen och förhandstillstånd inte kan erhållas i tid. Den myndighet som har ansvar för att ge förhandstillstånd ska underrättas utan dröjsmål.

3. Alla bestämmelser i detta kapitel ska tillämpas för att säkerställa att den skyddsnivå för fysiska personer som säkerställs genom detta direktiv inte undergrävs.

Artikel 36

Överföring på grundval av ett beslut om adekvat skyddsnivå

1. Medlemsstaterna ska föreskriva att 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 ett särskilt tillstånd.

2. När kommissionen bedömer om en adekvat skyddsnivå föreligger ska den särskilt beakta

a) rättsstatsprincipen, respekten för de mänskliga rättigheterna och grundläggande friheterna, relevant lagstiftning, både allmän lagstiftning och sektorslagstiftning, inklusive avseende allmän säkerhet, försvar, nationell säkerhet och straffrätt samt offentliga myndigheters tillgång till personuppgifter liksom tillämpningen av denna lagstiftning, dataskyddsregler, yrkesregler och säkerhetsbestämmelser och regler för vidare överföring av personuppgifter till ett annat tredjeland eller en annan internationell organisation, som ska följas i det tredjeland eller inom den internationella organisation som berörs, rättspraxis, och effektiva 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, med ansvar för att säkerställa och kontrollera att dataskyddsbestämmelserna följs, inklusive lämpliga verkställighetsbefogenheter, ge 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 skyddsnivån är adekvat, 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. Den territoriella och sektoriella tillämpningen 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 58.2.

4. Kommissionen ska fortlöpande övervaka utveckling i tredjeländer och internationella organisationer vilken kan påverka hur beslut som antagits enligt punkt 3 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 en adekvat skyddsnivå i den mening som avses i punkt 2 i den här artikeln och, i den mån det behövs, genom genomförandeakter dra tillbaka, 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 58.2.

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 58.3.

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. Medlemsstaterna ska föreskriva att ett beslut enligt punkt 5 inte ska påverka överföringar av personuppgifter till tredjelandet, territoriet eller en eller flera specificerade sektorer inom tredjelandet, eller den internationella organisationen i fråga, enligt artiklarna 37–38.

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 tredjeland samt de internationella organisationer för vilka den har fastställt att en adekvat skyddsnivå inte eller inte längre säkerställs.

Artikel 37

Överföring som omfattas av lämpliga skyddsåtgärder

1. Om det inte föreligger något beslut enligt artikel 36.3 ska medlemsstaterna föreskriva att en överföring av personuppgifter till ett tredjeland eller en internationell organisation får ske om

a) lämpliga skyddsåtgärder för personuppgifter har fastställts i ett rättsligt bindande instrument, eller

b) den personuppgiftsansvarige har bedömt alla omständigheter kring en överföring av personuppgifter och dragit slutsatsen att lämpliga skyddsåtgärder för personuppgifterna föreligger.

2. Den personuppgiftsansvarige ska informera tillsynsmyndigheten om kategorier av överföringar enligt punkt 1 b.

3. När en överföring grundas på punkt 1 b, ska denna överföring dokumenteras, och dokumentationen ska på begäran göras tillgänglig för tillsynsmyndigheten, inbegripet datum och tidpunkt för överföringen, information om den mottagande behöriga myndigheten, skälet till överföringen och de personuppgifter som har överförts.

Artikel 38

Undantag i särskilda situationer

1. Om det inte föreligger något beslut om adekvat skyddsnivå enligt artikel 36 eller lämpliga skyddsåtgärder enligt artikel 37, ska medlemsstaterna föreskriva att en överföring eller en kategori av överföringar av personuppgifter till ett tredjeland eller en internationell organisation får ske endast om överföringen är nödvändig

a) för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan person,

b) för att skydda den registrerades berättigade intressen, om lagstiftningen i den medlemsstat som överför personuppgifterna föreskriver detta,

c) för att avvärja en omedelbar och allvarlig fara för den allmänna säkerheten i en medlemsstat eller ett tredjeland,

d) i enskilda fall för de ändamål som anges i artikel 1.1. eller

e) i ett enskilt fall för att fastslå, göra gällande eller försvara rättsliga anspråk som hänför sig till de ändamål som anges i artikel 1.1.

2. Personuppgifter får inte överföras om den överförande behöriga myndigheten fastställer att den berörda registrerades grundläggande rättigheter och friheter väger tyngre än det allmänna intresset av en sådan överföring som avses i punkt 1 d och e.

3. När en överföring grundas på punkt 1, ska denna överföring dokumenteras, och dokumentationen ska på begäran göras tillgänglig för tillsynsmyndigheten, inbegripet datum och tidpunkt för överföringen, information om den mottagande behöriga myndigheten, skälet till överföringen och de personuppgifter som har överförts.

Artikel 39

Överföringar av personuppgifter till mottagare som är etablerade i tredjeländer

1. Genom undantag från artikel 35.1 b och utan att det påverkar tillämpningen av internationella avtal som avses i punkt 2 i den här artikeln, får det i unionsrätten eller medlemsstaternas nationella rätt föreskrivas att de behöriga myndigheter som avses i artikel 3.7 a, i enskilda och särskilda fall, får överföra personuppgifter direkt till mottagare som är etablerade i tredjeländer endast om de övriga bestämmelserna i detta direktiv efterlevs och samtliga följande villkor är uppfyllda:

a) Överföringen är absolut nödvändig för att utföra en uppgift som en överförande behörig myndighet ansvarar för i enlighet med unionsrätten eller medlemsstaternas nationella rätt för de ändamål som anges i artikel 1.1.

b) Den överförande behöriga myndigheten har fastställt att ingen av den berörda registrerades grundläggande rättigheter och friheter väger tyngre än det allmänna intresse som nödvändiggör överföringen i det aktuella fallet.

c) Den överförande behöriga myndigheten anser att överföring till en myndighet som är behörig för de ändamål som avses i artikel 1.1 i tredjelandet är ineffektivt eller olämpligt, i synnerhet eftersom överföringen inte kan göras inom rimlig tid.

d) Den myndighet i tredjelandet som är behörig för de ändamål som avses i artikel 1.1 har utan dröjsmål informerats, såvida detta inte är ineffektivt eller olämpligt.

e) Den överförande behöriga myndigheten har informerat mottagaren om det eller de specifika ändamål för vilka och personuppgifterna ska behandlas av den senare förutsatt att den behandlingen är nödvändig.

2. Med ett internationellt avtal som avses i punkt 1 avses varje gällande bilateralt eller multilateralt internationellt avtal mellan medlemsstater och tredjeländer inom området för straffrättsligt samarbete och polissamarbete.

3. Den överförande behöriga myndigheten ska informera tillsynsmyndigheten om överföringar enligt denna artikel.

4. Överföringar som grundar sig på punkt 1 ska dokumenteras.

Artikel 40

Internationellt samarbete för skydd av personuppgifter

När det gäller tredjeländer och internationella organisationer ska kommissionen och medlemsstaterna 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 41

Tillsynsmyndighet

1. Varje medlemsstat ska föreskriva att en eller flera offentliga myndigheter ska vara ansvariga för att övervaka tillämpningen av detta direktiv, i syfte att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandlingen samt att underlätta det fria flödet av sådana uppgifter inom unionen (*tillsynsmyndighet*).

2. Varje tillsynsmyndighet ska bidra till en enhetlig tillämpning av detta direktiv i hela unionen. För det ändamålet ska tillsynsmyndigheterna samarbeta såväl sinsemellan som med kommissionen i enlighet med kapitel VII.

3. Medlemsstaterna får föreskriva att en tillsynsmyndighet som har inrättats enligt förordning (EU) 2016/679 ska vara den tillsynsmyndighet som avses i detta direktiv och ta på sig ansvaret för de uppgifter som ska utföras av den tillsynsmyndighet som inrättas enligt punkt 1 i denna artikel.

4. Om det finns fler än en tillsynsmyndighet i en medlemsstat ska medlemsstaten utse den tillsynsmyndighet som ska företräda myndigheterna i fråga i den styrelse som avses i artikel 51.

Artikel 42

Oberoende

1. Varje medlemsstat ska föreskriva att varje tillsynsmyndighet ska vara fullständigt oberoende i utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med detta direktiv.

2. Medlemsstaterna ska föreskriva att dess tillsynsmyndigheters ledamot eller ledamöter i utförandet av sina uppgifter och i utövandet av sina befogenheter enligt detta direktiv ska stå fria från utomstående påverkan, direkt såväl som indirekt, och varken begära eller ta emot instruktioner av någon.

3. Medlemsstaternas tillsynsmyndigheters ledamot eller ledamöter ska avhålla sig 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 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 är 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 43

Allmänna villkor för tillsynsmyndighetens ledamöter

1. Medlemsstaterna ska föreskriva att varje ledamot av deras tillsynsmyndigheter ska utses genom ett öppet förfarande av

— deras parlament

— deras regering

— deras statschef, eller

— ett oberoende organ som enligt medlemsstaternas 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 de 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 nationella rätten i den berörda medlemsstaten.

4. En ledamot ska avsättas endast på grund av allvarlig försummelse eller när ledamoten inte längre uppfyller de krav som ställs för att kunna utföra sina uppgifter.

Artikel 44

Regler för inrättandet av en tillsynsmyndighet

1. Varje medlemsstat ska i lag fastställa samtliga följande:

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 6 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 rapporter från fysiska personer om överträdelser av detta direktiv.

Avsnitt 2

Behörighet, uppgifter och befogenheter

Artikel 45

Behörighet

1. Varje medlemsstat ska föreskriva att varje tillsynsmyndighet ska vara behörig att utföra de uppgifter och utöva de befogenheter som tilldelas den i enlighet med detta direktiv inom sin egen medlemsstats territorium.

2. Varje medlemsstat ska föreskriva att varje tillsynsmyndighet inte ska vara behörig att utöva tillsyn över domstolar som behandlar personuppgifter inom ramen för sin dömande verksamhet. Medlemsstaterna får föreskriva att deras tillsynsmyndighet inte ska vara behörig att utöva tillsyn över andra oberoende rättsliga myndigheter som behandlar personuppgifter inom ramen för sin rättsliga verksamhet.

Artikel 46

Uppgifter

1. Varje medlemsstat ska föreskriva att varje tillsynsmyndighet inom sitt territorium ska

a) övervaka och verkställa tillämpningen av de bestämmelser som antas i enlighet med detta direktiv och dess genomförandeåtgärder,

b) öka allmänhetens medvetenhet och kunskaper om risker, regler, skyddsåtgärder och rättigheter i samband med behandlingen,

c) i enlighet med medlemsstaternas nationella rätt ge rådgivning åt det nationella parlamentet, regeringen och andra institutioner och organ om lagstiftningsmässiga 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 detta direktiv,

e) på begäran tillhandahålla information till registrerade om hur de ska utöva sina rättigheter enligt detta direktiv, 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 55, 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) kontrollera att behandling enligt artikel 17 är laglig och inom en rimlig period informera den registrerade om resultatet av kontrollen enligt artikel 17.3 eller om skälen till att kontrollen inte har genomförts,

h) samarbeta, inbegripet genom att utbyta information, med och ge ömsesidigt bistånd till andra tillsynsmyndigheter för att se till att detta direktiv tillämpas och verkställs på ett enhetligt sätt,

i) utföra undersökningar om tillämpningen av detta direktiv, inbegripet på grundval av information som erhålls från en annan tillsynsmyndighet eller annan offentlig myndighet,

j) följa sådan utveckling som påverkar skyddet av personuppgifter, bland annat inom informations- och kommunikationsteknik,

k) ge råd om sådan behandling av personuppgifter som avses i artikel 28, och

l) bidra till styrelsens verksamhet.

2. Varje tillsynsmyndighet ska underlätta inlämningen av klagomål enligt punkt 1 f genom åtgärder, såsom att tillhandahålla 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 för dataskyddsombudet.

4. Om en begäran är uppenbart ogrundad eller orimlig, särskilt på grund av att den är repetitiv, 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 47

Befogenheter

1. Varje medlemsstat ska i lag säkerställa att varje tillsynsmyndighet har effektiva undersökningsbefogenheter. Dessa befogenheter ska minst inbegripa rätten att från den personuppgiftsansvarige och personuppgiftsbiträdet få tillgång till alla personuppgifter som behandlas och all information som tillsynsmyndigheten behöver för att kunna fullgöra sina uppgifter.

2. Varje medlemsstat ska i lag säkerställa att varje tillsynsmyndighet har effektiva korrigerande befogenheter, till exempel för att:

a) Utfärda varningar till den personuppgiftsansvarige eller personuppgiftsbiträdet om att planerade behandlingar sannolikt kommer att stå i strid med de bestämmelser som antas i enlighet med detta direktiv.

b) Beordra den personuppgiftsansvarige eller personuppgiftsbiträdet att se till att uppgiftsbehandlingen är förenlig med de bestämmelser som antas enligt detta direktiv, om lämpligt på ett visst sätt och inom en viss tid, bland annat genom att beordra rättelse, eller radering av personuppgifter eller begränsning av behandling enligt artikel 16.

c) Införa en tillfällig eller definitiv begränsning av, inklusive ett förbud mot, uppgiftsbehandlingen.

3. Varje medlemsstat ska i lag säkerställa att varje tillsynsmyndighet har effektiva befogenheter att ge den personuppgiftsansvarige råd i enlighet med det förfarande för förhandssamråd som avses i artikel 28 och att på eget initiativ eller på begäran avge yttranden till det nationella parlamentet, medlemsstatens regering eller, i enlighet med dess nationella rätt, till andra institutioner och organ samt till allmänheten, i frågor som rör skydd av personuppgifter.

4. Utövandet av de befogenheter som tillsynsmyndigheten tilldelas enligt denna artikel ska omfattas av lämpliga skyddsåtgärder, inbegripet effektiva rättsmedel och rättssäkerhet, som fastställts i unionsrätten och medlemsstaternas nationella rätt i enlighet med stadgan.

5. Varje medlemsstat ska i lag säkerställa att varje tillsynsmyndighet har befogenhet att göra rättsliga myndigheter uppmärksamma på överträdelser av de bestämmelser som antas i enlighet med detta direktiv och att, när så är lämpligt, inleda eller på annat sätt delta i rättsliga förfaranden, i syfte att säkerställa efterlevnaden av bestämmelser som antas i enlighet med detta direktiv.

Artikel 48

Rapportering av överträdelser

Medlemsstaterna ska föreskriva att de behöriga myndigheterna ska inrätta effektiva mekanismer för att uppmuntra till konfidentiell rapportering av överträdelser av detta direktiv.

Artikel 49

Verksamhetsrapport

Varje tillsynsmyndighet ska upprätta en årlig rapport om sin verksamhet, vilken kan omfatta en förteckning över typer av anmälda överträdelser och typer av ålagda sanktioner. Rapporterna ska översändas till det nationella parlamentet, regeringen och andra myndigheter som utsetts genom medlemsstaternas nationella rätt. Den ska göras tillgänglig för allmänheten, kommissionen och styrelsen.

KAPITEL VII

Samarbete

Artikel 50

Ömsesidigt bistånd

1. Medlemsstaterna ska föreskriva att tillsynsmyndigheterna ska utbyta relevant information och ge ömsesidigt bistånd i arbetet för att genomföra och tillämpa detta direktiv på ett enhetligt sätt, och ska införa åtgärder som bidrar till ett verkningsfullt samarbete. Det ömsesidiga biståndet ska särskilt omfatta begäranden om information och tillsynsåtgärder, till exempel begäranden om att genomföra samråd, inspektioner och utredningar.

2. Medlemsstaterna ska föreskriva att varje tillsynsmyndighet ska vidta alla lämpliga åtgärder för att kunna 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 och skälen till denna. Information som utbytts får endast användas för det syfte för vilket den har begärts.

4. En tillsynsmyndighet som tar emot begäran får bara 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 detta direktiv eller med den unionsrätt eller medlemsstatens nationella rätt som den tillsynsmyndighet som mottar begäran 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. Varje tillsynsmyndighet som tar emot 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 begäran får inte ta ut någon avgift för åtgärder som de vidtagit efter 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. 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. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 58.2.

Artikel 51

Styrelsens uppgifter

1. Styrelsen som inrättats genom förordning (EU) 2016/679 ska i samband med uppgiftsbehandling som omfattas av detta direktivs tillämpningsområde ha följande uppgifter:

a) Ge kommissionen råd i alla frågor som gäller skydd av personuppgifter inom unionen, till exempel om eventuella förslag till ändring av detta direktiv.

b) På eget initiativ, på begäran av en av sina ledamöter eller av kommissionen behandla frågor om tillämpningen av detta direktiv och utfärda riktlinjer, rekommendationer och bästa praxis i syfte att främja en enhetlig tillämpning av detta direktiv.

c) Utforma riktlinjer för tillsynsmyndigheterna i fråga om tillämpningen av de åtgärder som avses i artikel 47.1 och 47.3.

d) Utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led b i detta stycke för att konstatera personuppgiftsincidenter och fastställa det otillbörliga dröjsmål som avses i artikel 30.1 och 30.2 och för de särskilda omständigheter under vilka ett personuppgiftsbiträde eller en personuppgiftsansvarig är skyldig att anmäla personuppgiftsincidenten.

e) Utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led b i detta stycke angående de omständigheter under vilka en personuppgiftsincident sannolikt kommer att orsaka en hög risk för rättigheterna och friheterna för de fysiska personer som avses i artikel 31.1.

f) Se över den praktiska tillämpningen av de riktlinjer och rekommendationer samt den bästa praxis som avses i leden b och c.

g) Avge ett yttrande till kommissionen för bedömningen av huruvida skyddsnivån i ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom ett tredjeland, eller en internationell organisation är adekvat, inbegripet för en bedömning av huruvida det tredjelandet, det territoriet, den specificerade sektorn eller den internationella organisationen inte längre säkerställer en adekvat skyddsnivå.

h) Främja samarbete och effektivt bilateralt och multilateralt utbyte av bästa praxis och information mellan tillsynsmyndigheterna.

i) Främja gemensamma utbildningsprogram och underlätta personalutbyte mellan tillsynsmyndigheterna, och där så är lämpligt även med tillsynsmyndigheter i tredjeland och internationella organisationer.

j) Främja utbyte av kunskap och dokumentation om lagstiftning och bästa praxis på området för dataskydd med tillsynsmyndigheter med ansvar för dataskydd i hela världen.

Vad gäller första stycket led g ska kommissionen lämna all nödvändig dokumentation till styrelsen, inklusive korrespondens med regeringen i tredjelandet, med territoriet eller den specificerade sektorn i det tredjelandet eller med den internationella organisationen.

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 exempel på bästa praxis till kommissionen och till den kommitté som avses i artikel 58.1, samt offentliggöra dem.

4. Kommissionen ska hålla styrelsen underrättad om de åtgärder den vidtagit som en följd av styrelsens yttranden, riktlinjer, rekommendationer och bästa praxis.

KAPITEL VIII

Rättsmedel, ansvar och sanktioner

Artikel 52

Rätt att lämna in ett klagomål till en tillsynsmyndighet

1. Utan att det påverkar andra administrativa prövningsförfaranden eller rättsmedel ska medlemsstaterna föreskriva att alla registrerade personer som anser att behandling som avser dem står i strid med de bestämmelser som antas i enlighet med detta direktiv har rätt att lämna in ett klagomål till en enda tillsynsmyndighet.

2. Medlemsstaterna ska föreskriva att den tillsynsmyndighet som mottagit klagomålet ska överlämna det till den behöriga tillsynsmyndigheten utan onödigt dröjsmål, om klagomålet inte inlämnats till den myndighet som är behörig enligt artikel 45.1. Den registrerade ska informeras om överlämnandet.

3. Medlemsstaterna ska föreskriva att den tillsynsmyndighet som mottagit klagomålet ska tillhandahålla ytterligare hjälp på den registrerades begäran.

4. Den registrerade ska underrättas av den behöriga tillsynsmyndigheten om klagomålets handläggning och dess resultat, inbegripet rätten till rättsmedel enligt artikel 53.

Artikel 53

Rätt till ett effektivt rättsmedel mot en tillsynsmyndighets beslut

1. Utan att det påverkar något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol ska medlemsstater föreskriva att en fysisk eller juridisk person har rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut som avser dem och 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 enligt artikel 45.1 behöriga tillsynsmyndigheten inte inom tre månader behandlar ett klagomål eller om tillsynsmyndigheten inte informerar den registrerade om handläggningen eller resultatet av det klagomål som inlämnats enligt artikel 52.

3. Medlemsstaterna ska föreskriva att talan mot en tillsynsmyndighet ska väckas vid domstol i den medlemsstat där tillsynsmyndigheten har sitt säte.

Artikel 54

Rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde

Utan att det påverkar tillgängliga administrativa prövningsförfaranden eller prövningsförfaranden utanför domstol, inbegripet rätten att lämna in ett klagomål till en tillsynsmyndighet enligt artikel 52, ska medlemsstaterna föreskriva en rätt till effektiva rättsmedel för registrerade om han eller hon anser att deras rättigheter enligt de bestämmelser som antas enligt detta direktiv har kränkts som en följd av att hans eller hennes personuppgifter har behandlats på ett sätt som inte är förenligt med dessa bestämmelser.

Artikel 55

Företrädande av registrerade personer

Medlemsstaterna ska i enlighet med medlemsstaternas nationella processrätt se till att den registrerade har rätt att ge ett organ, en organisation eller en sammanslutning utan vinstsyfte som har inrättats på lämpligt sätt i enlighet med lagen i en medlemsstat, och vars stadgeenliga mål är av allmänt intresse och som är verksam inom området skydd av registrerades rättigheter och friheter vad gäller skyddet av deras personuppgifter, i uppdrag att lämna in klagomålet för hans eller hennes räkning och att utöva de rättigheter som avses i artiklarna 52, 53 och 54 för hans eller hennes räkning.

Artikel 56

Rätt till ersättning

Medlemsstaterna ska föreskriva att var och en som lidit materiell eller immateriell skada till följd av en olaglig behandling av personuppgifter eller av någon annan åtgärd som står i strid med de nationella bestämmelser som antas i enlighet med detta direktiv ska ha rätt till ersättning för denna skada från den personuppgiftsansvarige eller varje annan myndighet som är behörig enligt medlemsstaternas nationella rätt.

Artikel 57

Sanktioner

Medlemsstaterna ska föreskriva sanktioner för överträdelser av bestämmelser som antas enligt detta direktiv och ska vidta de åtgärder som krävs för att säkerställa att dessa sanktioner genomförs. Sanktionerna ska vara effektiva, proportionella och avskräckande.

KAPITEL IX

Genomförandeakter

Artikel 58

Kommittéförfarande

1. Kommissionen ska biträdas av den kommitté som inrättats enligt artikel 93 i förordning (EU) 2016/679. 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 den förordningen tillämpas.

KAPITEL X

Slutbestämmelser

Artikel 59

Upphävande av rambeslut 2008/977/RIF

1. Rambeslut 2008/977/RIF ska upphöra att gälla från och med den 6 maj 2018.

2. Hänvisningar till det upphävda beslut som avses i punkt 1 ska anses som hänvisningar till detta direktiv.

Artikel 60

Gällande unionsrättsakter

Detta direktiv ska inte påverka särskilda bestämmelser om skydd av personuppgifter i unionsrättsakter på området för straffrättsligt samarbete och polissamarbete som trädde i kraft den 6 maj 2016 eller tidigare, vilka reglerar behandling medlemsstaterna emellan och medlemsstaternas utsedda myndigheters tillgång till informationssystem som inrättats på grundval av fördragen och som är relevanta för detta direktivs tillämpningsområde.

Artikel 61

Förhållande till tidigare ingångna internationella avtal på området för straffrättsligt samarbete och polissamarbete

Internationella avtal som rör överföring av personuppgifter till tredjeländer eller internationella organisationer som ingicks av medlemsstaterna före den 6 maj 2016 och som är förenliga med unionsrätten så som den tillämpades före den dagen ska fortsätta att gälla tills de ändras, ersätts eller återkallas.

Artikel 62

Kommissionens rapporter

1. Kommissionen ska senast den 6 maj 2022 och därefter vart fjärde år överlämna en rapport om utvärderingen och översynen av detta direktiv till Europaparlamentet och rådet. Rapporten ska offentliggöras.

2. Inom ramen för de utvärderingar och översyner som avses i punkt 1 ska kommissionen i synnerhet granska tillämpningen av kapitel V om överföring av personuppgifter till tredjeländer och internationella organisationer samt hur bestämmelserna fungerar, och därvid särskilt beakta beslut som antagits i enlighet med artiklarna 36.3 och 39.

3. För de ändamål som avses i punkterna 1 och 2 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. Dessa rapporter får vid behov överlämnas tillsammans med lagstiftningsförslag om ändring, i syfte att ändra detta direktiv med särskild hänsyn till informationsteknikens utveckling och informationssamhällets framsteg.

6. Kommissionen ska senast den 6 maj 2019 se över andra rättsakter som antagits av unionen och som reglerar de behöriga myndigheternas behandling för att uppnå de mål som anges i artikel 1.1, inklusive de som avses i artikel 60, i syfte att bedöma om de behöver anpassas till detta direktiv och att, i förekommande fall, lägga fram förslag till ändring av dessa rättsakter för att säkerställa ett enhetligt tillvägagångssätt för skydd av personuppgifter inom detta direktivs tillämpningsområde.

Artikel 63

Införlivande

1. Medlemsstaterna ska senast den 6 maj 2018 anta och offentliggöra de lagar och andra författningar som är nödvändiga för att följa detta direktiv. De ska genast överlämna texten till dessa bestämmelser till kommissionen. De ska tillämpa dessa bestämmelser från och med den 6 maj 2018.

När en medlemsstat antar dessa bestämmelser ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda.

2. Genom undantag från punkt 1 får medlemsstaterna föreskriva att de automatiserade behandlingssystem som inrättades före den 6 maj 2016 undantagsvis, när det innebär oproportionella ansträngningar, ska bringas i överensstämmelse med artikel 25.1 senast den 6 maj 2023.

3. Genom undantag från punkterna 1 och 2 i denna artikel får en medlemsstat under exceptionella omständigheter bringa ett automatiserat behandlingssystem som avses i punkt 2 i denna artikel i överensstämmelse med artikel 25.1 inom en specifik tidsperiod efter den period som avses i punkt 2 i den här artikeln om det annars skulle uppstå allvarliga problem för driften av detta specifika automatiserade behandlingssystem. Den berörda medlemsstaten ska underrätta kommissionen om skälen till dessa allvarliga problem och skälen till den angivna tidsperioden inom vilken den ska bringa detta specifika automatiserade databehandlingssystem i överensstämmelse med artikel 25.1. Den angivna perioden ska under inga omständigheter inte vara senare än 6 maj 2026.

4. Medlemsstaterna ska till kommissionen överlämna texten till de centrala bestämmelser i medlemsstaternas nationella rätt som de antar inom det område som omfattas av detta direktiv.

Artikel 64

Ikraftträdande

Detta direktiv träder i kraft dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 65

Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Bryssel den 27 april 2016.

På Europaparlamentets vägnar	*På rådets vägnar*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT
Ordförande	*Ordförande*

Sammanfattning av betänkandet En ny kamerabevakningslag (SOU 2017:55)

Uppdraget

Utredningens uppdrag har varit att utreda vissa frågor om kameraövervakning enligt kameraövervakningslagen (2013:460). I uppdraget har även ingått att göra en analys av hur kameraövervakningslagen behöver anpassas till EU:s nya reglering om behandling av personuppgifter. EU-regleringen består av en förordning och ett direktiv. Direktivet gäller för personuppgiftsbehandling hos vissa myndigheter och andra för syften som avser bl.a. brottsbekämpning, lagföring och straffverkställighet medan förordningen omfattar annan personuppgiftsbehandling hos myndigheter och andra. Kameraövervakning utgör många gånger personuppgiftsbehandling och träffas därför av EU-regleringen. I direktiven till utredningen har det angetts att en strävan bör vara att behålla huvuddragen i den nuvarande lagen.

Kameraövervakningslagen tar sikte på viss kameraanvändning i samhället som sker öppet. Enligt lagen gäller som huvudregel ett krav på tillstånd för att kameraövervakning ska få ske av platser dit allmänheten har tillträde. Vidare finns ett krav på att det ska upplysas om kameraövervakning både vad gäller platser dit allmänheten har tillträde och vad gäller andra platser. Lagen reglerar inte s.k. hemlig kameraövervakning, som omfattas av annan lagstiftning.

I uppdraget har ingått att undersöka hur lagens tillämpningsområde förhåller sig till användning av ny teknik, såsom kamerautrustade drönare. Vad gäller brottsbekämpning har uppdraget varit att överväga om möjligheterna till kameraövervakning på särskilt brottsutsatta platser behöver förbättras, att analysera om andra relevanta aktörer än brottsbekämpande myndigheter har ändamålsenliga möjligheter till sådan övervakning och att bedöma om det finns tillräckliga möjligheter att ta hänsyn till hotbilder av mer generellt slag vid tillståndsprövningen enligt lagen. Uppdraget har dessutom innefattat bl.a. en analys av om integritetsskyddet på arbetsplatser behöver förbättras.

I utredningsuppdraget har inte ingått att överväga att avskaffa eller genomgripande förändra den särskilda lagstiftningen på kameraövervakningsområdet. Uppdraget har alltså inte omfattat att helt slopa det krav på tillstånd till kamerabevakning som gäller i dag eller att ta bort eller avsevärt begränsa den skyldighet att upplysa om kameraövervakning som finns i dag. I uppdraget har inte heller ingått att helt undanta vissa rättssubjekt från lagstiftningens tillämpningsområde eller från tillståndskravet och upplysningskravet. Det har vidare inte ingått i uppdraget att överväga utvidgningar i annan lagstiftning som reglerar kameraanvändning, t.ex. att föreslå ökade möjligheter för polisen att bedriva hemlig kameraövervakning enligt rättegångsbalken eller lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

Med anledning av den nya EU-regleringen har det ändå övervägts varför en fortsatt särskild svensk lagstiftning på kameraövervakningsområdet är

motiverad och prövats vilka svenska bestämmelser som är tillåtna enligt EU-regleringen och huruvida dessa bestämmelser också är påkallade av principiella och praktiska skäl. Övervägandena har gjorts i ljuset av det beskrivna innehållet i uppdraget.

Uppdraget har genomförts med beaktande av det arbete som utförts av två andra utredningar, vilka haft i uppdrag att föreslå de nya generella svenska författningar som förordningen och direktivet kräver. De utredningarna har föreslagit en lag som kompletterar förordningen, dataskyddslagen, och föreskrifter till denna respektive en lag som genomför direktivet, brottsdatalagen, och föreskrifter till denna. Vidare har kontakter skett även med andra utredningar, som på olika områden överväger vilka förändringar som EU-regleringen och de nya generella författningarna ger anledning till. Dessutom har ett flertal möten ägt rum med myndigheter och andra som berörs av de frågor som uppdraget omfattat.

En ny kamerabevakningslag

I betänkandet föreslås att kameraövervakningslagen ska ersättas av en ny lag, som ska heta kamerabevakningslagen. Lagen ska träda i kraft den 25 maj 2018.

Skälen för att en helt ny lag föreslås är följande. Den nya EU-förordningen kommer att gälla direkt i Sverige, vilket innebär att bestämmelser om kameraövervakning som upprepar eller avviker från innehållet i förordningen inte kan behållas i svensk lagstiftning annat än om förordningen lämnar utrymme för det. Många av kameraövervakningslagens bestämmelser kan inte behållas alls eller kan inte behållas i sin nuvarande form när det gäller kameraövervakning som omfattas av förordningen. Vad gäller det nya EU-direktivet ska detta genomföras i svensk rätt. Svenska bestämmelser som omfattar kameraövervakning som träffas av direktivet måste uppfylla direktivets krav. Kraven uppfylls dock endast delvis av kameraövervakningslagens bestämmelser. Vidare har en utvärdering av kameraövervakningslagen som utredningen gjort visat att det finns vissa tillämpningssvårigheter med lagen. Sammantaget innebär detta att det krävs en stor reform av den svenska lagstiftningen på området för kameraövervakning.

Som utgångspunkter för kamerabevakningslagen har slagits fast att den – jämfört med kameraövervakningslagen – bör ge ökade möjligheter till kamerabevakning både för brottsbekämpande ändamål och för andra berättigade ändamål, t.ex. ändamål som avser kamerabevakning inom jordbruk och skogsbruk samt annan näringsverksamhet, och samtidigt ge ett förstärkt skydd för den personliga integriteten vid kamerabevakning, bl.a. på arbetsplatser.

Kamerabevakningslagens syfte ska vara att tillgodose behovet av kamerabevakning för berättigade ändamål och att skydda enskilda mot otillbörliga intrång i den personliga integriteten vid sådan bevakning.

Lagen ska endast innehålla de bestämmelser som särskilt behövs för kamerabevakning till skillnad mot annan behandling av personuppgifter som omfattas av EU-regleringen.

I frågor som inte regleras i lagen ska gälla antingen förordningen och dataskyddslagen med föreskrifter eller brottsdatalagen med föreskrifter beroende på om kamerabevakningen i det enskilda fallet omfattas av förordningen eller dataskyddslagen eller av brottsdatalagen.

Kamerabevakningslagen ska ha ett förhållandevis brett tillämpningsområde. Med kamerabevakning ska förstås att kameror eller därmed jämförbara utrustningar, utan att manövreras på platsen, används varaktigt eller regelbundet upprepat för personbevakning. Med personbevakning menas att människor kan identifieras genom bevakningen. Så är t.ex. fallet om hela personen eller personens ansikte syns tydligt. Om en människa endast av en tillfällighet kan hamna i en kameras blickfång, är det inte fråga om personbevakning. Även separata tekniska anordningar för avlyssning eller upptagning av ljud, som används för personbevakning, ska omfattas av begreppet kamerabevakning. Dessutom ska användning av separata tekniska anordningar för att behandla upptaget bild- och ljudmaterial omfattas.

Exempel på kameraanvändning som i regel inte ska träffas av lagen är användning av handhållna kameror och kameror som på annat sätt bärs på kroppen. Lagen ska inte heller omfatta t.ex. en kamera som är placerad på vindrutan i en bil eller monterad på ett cykelstyre när användaren av kameran är i kamerans omedelbara närhet och fortlöpande styr över denna. Däremot ska lagen omfatta kameror på drönare och på eller i bussar, tågvagnar och liknande objekt förutsatt att kamerorna inte manövreras på platsen. Lagen ska också omfatta kameror som är placerade på eller inuti byggnader, på stolpar och på liknande geografiskt bestämda platser.

Lagen ska endast gälla om de kameror eller separata ljudanordningar som används finns i Sverige och den som bedriver bevakningen är etablerad här eller i tredjeland. Vad gäller separata anordningar för att behandla material från sådan bevakning ska lagen gälla så länge behandlingen utförs av samma person som tagit upp materialet eller för dennes räkning.

Från lagen ska undantas kamerabevakning som en fysisk person utför som ett led i en verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll. Vidare ska hemlig kameraövervakning undantas. Dessutom ska undantag göras för kamerabevakning som sker i en verksamhet som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen och kamerabevakning som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

Sådan kameraanvändning som faller utanför lagens tillämpningsområde kan i stället omfattas av andra bestämmelser, främst bestämmelserna i förordningen och dataskyddslagen eller bestämmelserna i brottsdatalagen.

Ett upplysningskrav

I lagen ska – i likhet med kameraövervakningslagen – finnas ett krav på att det ska lämnas upplysning om kamerabevakning. Upplysningskravet ska gälla oavsett vem som bedriver kamerabevakningen och oavsett om bevakningen avser en plats dit allmänheten har tillträde eller en annan plats. Kravet ska delvis vara strängare än tidigare. Den som bedriver

kamerabevakning ska genom tydlig skyltning eller på något annat liknande verksamt sätt lämna upplysning om bevakningen, sin identitet och sina kontaktuppgifter och kontaktuppgifter till ett eventuellt dataskyddsombud. Om ljud kan avlyssnas eller tas upp vid bevakningen, ska en särskild upplysning lämnas om detta. Dessutom ska viss ytterligare information göras tillgänglig, t.ex. via en webbsida. Det gäller bl.a. information om ändamålet med kamerabevakningen och möjligheten att lämna in klagomål till tillsynsmyndigheten och kontaktuppgifterna till den myndigheten.

Från upplysningskravet ska gälla vissa undantag. Några av dessa har gällt även enligt den tidigare lagen och några är nya. De nya undantagen avser kamerabevakning som bedrivs i brådskande fall från ett luftfartyg, t.ex. en drönare. Det ena undantaget gäller när sådan bevakning bedrivs av Polismyndigheten eller Säkerhetspolisen i ett fall där det av särskild anledning finns risk för viss allvarlig brottslighet och syftet med bevakningen är att förebygga, förhindra, upptäcka, utreda eller lagföra denna. Det andra undantaget gäller när bevakning bedrivs av Polismyndigheten eller den som är räddningsledare enligt lagen (2003:778) om skydd mot olyckor i ett fall där bevakningen är av vikt för att avvärja en hotande olycka eller begränsa verkningarna av en inträffad olycka.

I enskilda fall ska dessutom tillsynsmyndigheten kunna besluta om undantag från upplysningskravet, om det finns synnerliga skäl för det. Ett sådant beslut ska kunna ändras eller återkallas vid ändrade förhållanden.

Ökade möjligheter till kamerabevakning – ett begränsat tillståndskrav

Kamerabevakningslagen ska – till skillnad mot kameraövervakningslagen – inte innehålla något generellt krav på tillstånd för att kamerabevakning ska få ske. Inte heller ska lagen innehålla något krav på anmälan som motsvarar den gamla lagens anmälningsskyldighet. Däremot ska den nya lagen innehålla ett begränsat tillståndskrav.

Eftersom en utgångspunkt för lagen är att den bör ge ökade möjligheter till kamerabevakning, finns det redan av den anledningen skäl att ifrågasätta om det är motiverat att behålla ett allmänt krav på tillstånd. Vidare innebär EU-regleringen att det inte längre är möjligt att upprätthålla en generell tillståndsplikt för sådan kamerabevakning som omfattas av förordningen. Förordningen tillåter endast krav på tillstånd i vissa fall. För kamerabevakning som träffas av direktivet kan däremot ett generellt sådant krav gälla.

Genom att slopa dagens generella tillståndskrav och anmälningsskyldighet kommer kamerabevakning i många verksamheter framöver att bli tillstånds- och anmälningsfri. Därmed kan möjligheterna att bedriva kamerabevakning i dessa verksamheter öka. Även om andra bestämmelser ska gälla för sådan kamerabevakning kan det förutses att den svenska tillsynsmyndigheten på området, liksom svenska domstolar och ytterst EU-domstolen, kommer att ha en mer generös syn på utrymmet för kamerabevakning än vad som hittills gällt enligt svensk rätt. Rättsläget är helt nytt med den nya EU-regleringen. Den skiljer sig i olika delar från den

unionsrättsliga reglering som fram till nu har gällt på området och legat till grund för dagens kameraövervakningslag. Exempelvis kan fler berättigade ändamål åberopas enligt den nya regleringen för att kamerabevakning ska få ske.

Även det tillståndskrav som kamerabevakningslagen ska innehålla därför att principiella och praktiska skäl motiverar det kan förenas med ökade möjligheter till kamerabevakning. Tillståndsförfarandet innebär en prövning enligt vissa i lagen på förhand givna kriterier, som är särskilt anpassade för de behov och de integritetsaspekter som gör sig gällande just på kamerabevakningsområdet. Kriterierna kan främja att prövningen blir förutsebar och enhetlig samt att tillstånd beviljas i en större omfattning än vad som varit fallet enligt kameraövervakningslagen i motsvarande situationer. Tillsynsmyndighetens beslut i en sådan fråga ska kunna överklagas till domstol. När ett tillstånd har meddelats kan tillståndshavaren inrätta sig efter detta.

Utan ett tillståndsförfarande skulle mer allmänna bestämmelser i förordningen eller de generella svenska författningarna gälla. Det skulle innebära att den som vill bedriva kamerabevakning ska göra en konsekvensbedömning av den planerade bevakningen i vissa fall och eventuellt samråda med tillsynsmyndigheten, som kan ingripa mot – t.ex. förbjuda – denna. I så fall finns det en risk för att rättsläget kommer att vara osäkert under en längre tid vad gäller sådana verksamheter som tillståndskravet annars kan avse. Det finns också en risk för att rättspraxis inte utvecklas på ett sätt som säkerställer att kamerabevakning kan användas i dessa verksamheter i situationer där sådan bevakning måste anses behövlig.

För kamerabevakning som ska omfattas av tillståndskravet ska den nya lagen ge ökade möjligheter att få tillstånd dels genom att de intressen av kamerabevakning som ska tillmätas betydelse vid tillståndsprövningen utökas jämfört med den gamla lagen, dels genom att undantagen från tillståndskravet vidgas något jämfört med den lagen.

Tillståndskravet ska gälla endast för vissa subjekt och för platser dit allmänheten har tillträde. Kravet ska gälla för myndigheter, både statliga och kommunala. Det ska också gälla för andra juridiska personer eller fysiska personer när de utför en uppgift som följer av lag eller annan författning, kollektivavtal eller beslut som meddelats med stöd av lag eller annan författning, om uppgiften avser brottsbekämpning, lagföring, straffverkställighet, upprätthållande av allmän ordning och säkerhet eller nationell säkerhet eller om uppgiften annars är av allmänt intresse.

Kravet på tillstånd till kamerabevakning ska alltså träffa samtliga myndigheter, i den mån viss bevakning som dessa bedriver inte är undantagen från kravet, och dessutom privaträttsliga subjekt som driver exempelvis skolverksamhet, kollektivtrafik, hälso- och sjukvård och förläggningar för asylsökande.

Tillståndskravet ska däremot inte gälla t.ex. privaträttsliga subjekts kamerabevakning i butikslokaler, av medieredaktioner, av lokaler som används av religiösa samfund och av idrottsarenor. Inte heller ska det omfatta exempelvis kamerabevakning inom jordbruk och skogsbruk eller av vilt, t.ex. vid åtlar. I dessa fall ska inte heller gälla någon anmälningsskyldighet.

Från kravet på tillstånd ska gälla vissa undantag som i huvudsak motsvarar undantagen från tillståndsplikten enligt kameraövervakningslagen. Några av den lagens undantag ska vidgas. Exempelvis undantas kamerabevakning som bedrivs under högst en månads tid av Polismyndigheten eller Säkerhetspolisen när det av särskild anledning finns risk för viss allvarlig brottslighet och syftet med bevakningen är att förebygga, förhindra, upptäcka, utreda eller lagföra denna. Vidare ska undantas viss kamerabevakning som hittills varit anmälningsskyldig, t.ex. bevakning i tunnelbanan.

Tillstånd till kamerabevakning ska ges om intresset av sådan bevakning väger tyngre än den enskildes intresse av att inte bli bevakad. Vid bedömningen av intresset av kamerabevakning ska det särskilt beaktas om bevakningen behövs för att

förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott på en brottsutsatt plats,

förebygga, förhindra, upptäcka, utreda eller lagföra angrepp på någons liv, hälsa eller trygghet till person eller på egendom på en plats där det av särskild anledning finns risk för sådana angrepp,

förebygga, förhindra eller upptäcka störningar av allmän ordning och säkerhet eller begränsa verkningarna av sådana störningar,

utöva kontrollverksamhet,

förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor, eller

tillgodose andra därmed jämförliga ändamål.

Vid ändrade förhållanden ska ett tillstånd kunna ändras eller återkallas.

Ett förstärkt integritetsskydd på arbetsplatser

I fråga om kamerabevakning på arbetsplatser som ska omfattas av kravet på tillstånd till sådan bevakning ska – liksom enligt kameraövervakningslagen – ett yttrande från ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på arbetsplatsen lämnas in tillsammans med en ansökan om tillstånd. Detsamma ska gälla i fråga om en ansökan om undantag från upplysningskravet vid kamerabevakning på arbetsplatser.

När det gäller kamerabevakning på arbetsplatser som inte ska omfattas av tillståndskravet ska införas en ny skyldighet för arbetsgivaren att först förhandla om bevakningen med en organisation som företräder arbetstagarna på arbetsplatsen. Förhandlingsskyldigheten ska fullgöras på det sätt som anges i lagen (1976:580) om medbestämmande i arbetslivet. Från förhandlingsskyldigheten ska avvikelse få göras genom kollektivavtal.

En organisation som företräder arbetstagarna på arbetsplatsen ska ha rätt att överklaga beslut om tillstånd till kamerabevakning och beslut om undantag från upplysningskravet.

Ett förstärkt integritetsskydd i övrigt

Vid kamerabevakning ska i övrigt gälla de bestämmelser som finns i förordningen och dataskyddslagen med föreskrifter eller brottsdatalagen med föreskrifter och som avser principer för behandling av personuppgifter, rättigheter för enskilda, skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden samt överföring av personuppgifter till tredjeland eller internationella organisationer. Att låta dessa bestämmelser gälla för kamerabevakning ger ett förstärkt integritetsskydd jämfört med vad som gällt hittills.

Tillsyn, sanktioner och rättsmedel

Tillsynen över kamerabevakning ska samlas hos en enda myndighet, Datainspektionen, och inte längre vara uppdelad mellan länsstyrelserna och Datainspektionen.

I ett ärende enligt kamerabevakningslagen hos tillsynsmyndigheten ska bestämmelser om undersökningsbefogenheter för den myndigheten i förordningen och dataskyddslagen med föreskrifter eller i brottsdatalagen med föreskrifter tillämpas. Vid underlåtenhet att bistå tillsynsmyndigheten i ett sådant ärende ska bestämmelser om sanktionsavgifter tillämpas. Bestämmelserna om sanktionsavgifter ska även tillämpas vid överträdelser av kamerabevakningslagen eller av beslut som meddelats med stöd av lagen. Vid sådana överträdelser ska dessutom bestämmelser om skadestånd tillämpas.

Något straffansvar för den som bryter mot kamerabevakningslagen eller beslut som meddelats med stöd av lagen ska inte längre kunna följa.

Tillsynsmyndighetens beslut enligt lagen, t.ex. i frågor om tillstånd till kamerabevakning, undantag från kravet på upplysning om kamerabevakning och sanktionsavgifter, ska få överklagas till allmän förvaltningsdomstol. Beslut om tillstånd till kamerabevakning och om undantag från upplysningskravet ska få överklagas även av den kommun där bevakningen ska ske. Som framgått ovan ska ett sådant beslut – när kamerabevakningen ska avse en arbetsplats – också få överklagas av en organisation som företräder arbetstagarna på arbetsplatsen.

I övrigt ska bestämmelser om tillsynsmyndighetens befogenheter, sanktioner, överklagande m.m. i förordningen och dataskyddslagen med föreskrifter eller i brottsdatalagen med föreskrifter gälla för kamerabevakning såvitt avser ärenden, beslut, överträdelser m.m. som inte regleras direkt i kamerabevakningslagen.

Betänkandets lagförslag

Förslag till kamerabevakningslag

Härigenom föreskrivs följande.

Allmänna bestämmelser

Inledande bestämmelse

1 § I denna lag finns bestämmelser om kamerabevakning som

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

– genomför 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, nedan kallat dataskyddsdirektivet, eller

– avser sådan kamerabevakning som inte omfattas av dataskydds-förordningen eller dataskyddsdirektivet.

Lagens syfte

2 § Syftet med denna lag är att tillgodose behovet av kamerabevakning för berättigade ändamål och att skydda enskilda mot otillbörliga intrång i den personliga integriteten vid sådan bevakning.

Lagens tillämpningsområde

3 § Denna lag gäller vid kamerabevakning. Med kamerabevakning förstås

1. att en TV-kamera, ett annat optisk-elektroniskt instrument eller en därmed jämförbar utrustning, utan att manövreras på platsen, används varaktigt eller regelbundet upprepat för personbevakning,

2. att en separat teknisk anordning för avlyssning eller upptagning av ljud används för personbevakning i samband med användning av sådan utrustning som avses i 1, och

3. att en separat teknisk anordning för att behandla upptaget bild- och ljudmaterial används.

4 § Lagen gäller endast om

1. kamerabevakning enligt 3 § 1 eller 2 sker med utrustning som finns i Sverige och den som bedriver bevakningen är etablerad i Sverige eller i tredjeland, eller

2. kamerabevakning enligt 3 § 3 avser behandling av bild- och ljudmaterial som tagits upp vid bevakning som avses i 1 och behandlingen utförs av den som bedriver bevakningen eller för hans eller hennes räkning.

5 § Lagen gäller inte vid

1. kamerabevakning som en fysisk person utför som ett led i en verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll,
2. hemlig kameraövervakning enligt 27 kap. rättegångsbalken eller lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott,
3. kamerabevakning som sker i en verksamhet som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen, och
4. kamerabevakning som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

Lagens förhållande till andra bestämmelser

6 § Utöver vad som föreskrivs i denna lag gäller i tillämpliga delar

1. dataskyddsförordningen, lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning, föreskrifter som meddelats med stöd av den lagen eller annan författning som kompletterar dataskyddsförordningen vid kamerabevakning som omfattas av förordningen eller den angivna lagen, eller
2. brottsdatalagen (2018:000), föreskrifter som meddelats med stöd av den lagen eller annan författning som genomför dataskyddsdirektivet vid kamerabevakning som omfattas av brottsdatalagen.

Uttryck i lagen

7 § Uttryck som används i denna lag har samma betydelse som i dataskyddsförordningen när det gäller kamerabevakning som omfattas av förordningen eller lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning eller som i brottsdatalagen (2018:000) när det gäller kamerabevakning som omfattas av den lagen.

Tillstånd till kamerabevakning

Krav på tillstånd

8 § Tillstånd krävs till kamerabevakning av en plats dit allmänheten har tillträde, om bevakningen ska bedrivas av en myndighet. Detsamma gäller om kamerabevakning av en sådan plats ska bedrivas av en annan juridisk person eller en fysisk person vid utförande av en uppgift som följer av lag eller annan författning, kollektivavtal eller beslut som meddelats med stöd av lag eller annan författning och

1. avser brottsbekämpning, lagföring eller straffverkställighet eller upprätthållande av allmän ordning och säkerhet,
2. avser nationell säkerhet, eller
3. annars är av allmänt intresse.

9 § Tillstånd till kamerabevakning ska ges om intresset av sådan bevakning väger tyngre än den enskildes intresse av att inte bli bevakad.

Vid bedömningen av intresset av kamerabevakning ska det särskilt beaktas om bevakningen behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott på en brottsutsatt plats eller på en annan plats där det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet till person eller på egendom,

2. förebygga, förhindra eller upptäcka störningar av allmän ordning och säkerhet eller begränsa verkningarna av sådana störningar,

3. utöva kontrollverksamhet,

4. förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor, eller

5. tillgodose andra därmed jämförliga ändamål.

Vid bedömningen av den enskildes intresse av att inte bli kamerabevakad ska det särskilt beaktas

1. hur bevakningen ska utföras,

2. om teknik som främjar skyddet av den enskildes personliga integritet ska användas, och

3. vilket område som ska bevakas.

Undantag från tillståndskravet

10 § Tillstånd till kamerabevakning krävs inte vid

1. bevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning,

2. bevakning som sker för att skydda en byggnad, en annan anläggning eller ett område som enligt 4 § 4, 5 § 1–4 eller 6 § första stycket skyddslagen (2010:305) har förklarats vara skyddsobjekt, om bevakningen endast omfattar skyddsobjektet eller ett område i dess omedelbara närhet,

3. bevakning som Försvarsmakten bedriver från ett fordon, fartyg eller luftfartyg som ett led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan bevakning,

4. bevakning som Trafikverket bedriver

a) av vägtrafik eller av sjötrafik vid en rörlig bro,

b) vid en betalstation som avses i bilagorna till lagen (2004:629) om trängselskatt och som sker för att samla in endast uppgifter som behövs för att beslut om trängselskatt ska kunna fattas och för att kontrollera att sådan skatt betalas, och

c) vid en betalstation på allmän väg som används vid uttag av infrastrukturavgifter enligt lagen (2014:52) om infrastrukturavgifter på väg och som sker för att samla in endast uppgifter som behövs för att beslut om infrastrukturavgift ska kunna fattas och för att kontrollera att sådan avgift betalas,

5. sådan trafikbevakning i en vägtunnel som avses i lagen (2006:418) om säkerhet i vägtunnlar och som bedrivs av någon annan tunnelhållare än Trafikverket,

6. bevakning i en tunnelbanevagn eller av en tunnelbanestation, om bevakningen har till enda syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott eller förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor,

7. bevakning i en lokal där det bedrivs postverksamhet eller av området omedelbart utanför in- och utgångar till en sådan lokal eller av en yta i en

butikslokal på vilken det bedrivs postverksamhet, om bevakningen har till enda syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott,

8. bevakning i ett parkeringshus, om bevakningen har till enda syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott, och

9. bevakning som sker för säkerheten i trafiken eller arbetsmiljön från ett fordon, en maskin eller liknande för att förbättra sikten för föraren eller användaren.

Undantaget från tillståndskravet i första stycket 2 gäller inte för sådana byggnader, andra anläggningar och områden som används för eller är avsedda för fredstida krishantering enligt 4 § 4 skyddslagen.

Tillfälliga undantag från tillståndskravet

11 § Kamerabevakning får ske under högst en månad utan att en ansökan om tillstånd har gjorts vid

1. bevakning som bedrivs av Polismyndigheten eller Säkerhetspolisen, om det av särskild anledning finns risk för allvarlig brottslighet som innebär fara för liv eller hälsa eller för omfattande förstörelse av egendom på en viss plats och syftet med bevakningen är att förebygga, förhindra eller upptäcka sådan brottslig verksamhet eller utreda eller lagföra sådana brott,

2. bevakning som bedrivs av Polismyndigheten eller den som är räddningsledare enligt lagen (2003:778) om skydd mot olyckor, om bevakningen är av vikt för att avvärja en hotande olycka eller begränsa verkningarna av en inträffad olycka, och

3. bevakning som bedrivs av den som är räddningsledare enligt lagen om skydd mot olyckor, om bevakningen är av vikt för att efterforska en försvunnen person.

Om en ansökan om tillstånd görs inom en månad från det att kamerabevakningen inleddes, får bevakningen bedrivas utan tillstånd till dess att ansökningen har prövats.

Ansökan om tillstånd

12 § En ansökan om tillstånd till kamerabevakning ska göras skriftligen hos tillsynsmyndigheten.

Ansökningen ska innehålla

1. uppgift om den som ska bedriva bevakningen och i förekommande fall den som ska ha hand om bevakningen för tillståndshavarens räkning,

2. uppgift om bevakningens ändamål,

3. en beskrivning av bevakningen, särskilt den utrustning som ska användas, var utrustningen ska placeras, det område som ska bevakas och de tider då bevakning ska ske,

4. en bedömning av behovet av och proportionaliteten i bevakningen i förhållande till ändamålet,

5. en bedömning av riskerna för intrång i den personliga integriteten och en beskrivning av de åtgärder som planeras för att hantera riskerna, och

6. uppgift om de omständigheter i övrigt som är av betydelse för prövningen av ärendet.

Om bevakningen avser en arbetsplats, ska ett yttrande från ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på arbetsplatsen lämnas in tillsammans med ansökningen.

Yttrande av kommunen

13 § Innan tillsynsmyndigheten beslutar om tillstånd till kamerabevakning ska den kommun där bevakningen ska ske få tillfälle att yttra sig, om det behövs.

Beslut om tillstånd

14 § Ett beslut om tillstånd till kamerabevakning ska ange vem som ska bedriva bevakningen och i förekommande fall vem som ska ha hand om bevakningen för tillståndshavarens räkning.

Beslutet ska förenas med villkor om hur kamerabevakningen får anordnas. Villkoren ska avse

1. bevakningens ändamål,
2. den utrustning som får användas och var utrustningen får placeras,
3. det område som får bevakas och de tider då bevakning får ske, och
4. upplysning om bevakningen, behandling av bilder eller ljud och andra förhållanden som har betydelse för att skydda enskildas personliga integritet, om sådana villkor behövs för tillståndet.

Ett tillstånds giltighet får begränsas till en viss tid.

15 § Om förutsättningarna för ett tillstånd ändras, får tillsynsmyndigheten besluta om nya villkor eller, om förutsättningarna för tillstånd inte längre är uppfyllda, återkalla tillståndet.

Upplysning om kamerabevakning

Krav på upplysning

16 § Vid kamerabevakning ska genom tydlig skyltning eller på något annat liknande verksamt sätt lämnas upplysning om

1. kamerabevakningen,
2. identiteten hos och kontaktuppgifterna till den som ska bedriva bevakningen, och
3. kontaktuppgifter till ett eventuellt dataskyddsombud.

Om ljud kan avlyssnas eller tas upp vid bevakningen, ska en särskild upplysning lämnas om detta.

Information ska även göras tillgänglig för dem som kan bli kamerabevakade om

1. ändamålet med och den rättsliga grunden för kamerabevakningen,
2. hur länge upptaget bild- och ljudmaterial får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa detta, och
3. möjligheten att lämna in klagomål till tillsynsmyndigheten och kontaktuppgifterna till den.

Undantag från upplysningskravet

17 § Upplysning om kamerabevakning behöver inte lämnas vid

1. bevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning,

2. bevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller Säkerhetspolisen, om det av särskild anledning finns risk för allvarlig brottslighet som innebär fara för liv eller hälsa eller för omfattande förstörelse av egendom på en viss plats och syftet med bevakningen är att förebygga, förhindra eller upptäcka sådan brottslig verksamhet eller utreda eller lagföra sådana brott,

3. bevakning som sker för att skydda en byggnad, en annan anläggning eller ett område som enligt 4 § 4, 5 § 1–4 eller 6 § första stycket skyddslagen (2010:305) har förklarats vara skyddsobjekt, om bevakningen endast omfattar skyddsobjektet eller ett område i dess omedelbara närhet,

4. bevakning som Försvarsmakten bedriver från ett fordon, fartyg eller luftfartyg som ett led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan bevakning,

5. bevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller den som är räddningsledare enligt lagen (2003:778) om skydd mot olyckor, om bevakningen är av vikt för att avvärja en hotande olycka eller begränsa verkningarna av en inträffad olycka, och

6. bevakning som bedrivs av den som är räddningsledare enligt lagen om skydd mot olyckor, om bevakningen är av vikt för att efterforska en försvunnen person.

Undantaget från upplysningskravet i första stycket 3 gäller inte för sådana byggnader, andra anläggningar eller områden som används för eller är avsedda för fredstida krishantering enligt 4 § 4 skyddslagen.

18 § Undantagen från upplysningskravet gäller inte, om ljud ska avlyssnas eller tas upp vid kamerabevakningen.

Undantag från upplysningskravet i enskilda fall

19 § Om det finns synnerliga skäl, får tillsynsmyndigheten i enskilda fall besluta om undantag från upplysningskravet.

Ansökan om undantag

20 § En ansökan om undantag från upplysningskravet ska göras skriftligen hos tillsynsmyndigheten.

Ansökningen ska innehålla uppgift om den som ska bedriva kamerabevakningen och i förekommande fall den som ska ha hand om bevakningen för hans eller hennes räkning samt skälen för ansökningen.

Om bevakningen avser en arbetsplats, ska ett yttrande från ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på arbetsplatsen lämnas in tillsammans med ansökningen.

Yttrande av kommunen

21 § Innan tillsynsmyndigheten beslutar om undantag från upplysningskravet ska den kommun där kamerabevakningen ska ske få tillfälle att yttra sig, om bevakningen ska avse en plats dit allmänheten har tillträde och det behövs ett yttrande.

Beslut om undantag

22 § Ett beslut om undantag från upplysningskravet ska ange vem som ska bedriva kamerabevakningen och i förekommande fall vem som ska ha hand om bevakningen för hans eller hennes räkning.

Beslutet ska förenas med de villkor som behövs.

23 § Om förutsättningarna för ett beslut om undantag ändras, får tillsynsmyndigheten ändra beslutet eller, om förutsättningarna för ett sådant beslut inte längre är uppfyllda, återkalla detta.

Förhandlingsskyldighet för arbetsgivare

Förhandlingsskyldighet

24 § Innan en arbetsgivare beslutar om kamerabevakning som avser arbetsplatsen och som inte omfattas av kravet på tillstånd ska arbetsgivaren förhandla med berörd arbetstagarorganisation på det sätt som anges i 11–14 §§ lagen (1976:580) om medbestämmande i arbetslivet.

Undantag från förhandlingsskyldigheten

25 § Från förhandlingsskyldigheten för arbetsgivare får avvikelse göras genom kollektivavtal.

Tystnadsplikt och utlämnande av uppgifter

26 § Den som tar befattning med en uppgift som har inhämtats genom kamerabevakning får inte obehörigen röja eller utnyttja det som han eller hon på detta sätt har fått veta om någon enskilds personliga förhållanden. I det allmännas verksamhet tillämpas i stället bestämmelserna i offentlighets- och sekretesslagen (2009:400).

Tillsyn, sanktionsavgifter och skadestånd

Tillsynsmyndighet

27 § Den myndighet som regeringen bestämmer (tillsynsmyndigheten) utövar tillsyn över kamerabevakning enligt denna lag.

Undersökningsbefogenheter, sanktionsavgifter och skadestånd

28 § I ett ärende enligt denna lag hos tillsynsmyndigheten och vid underlåtenhet att bistå den myndigheten i ett sådant ärende tillämpas bestämmelser om undersökningsbefogenheter för tillsynsmyndigheten och sanktionsavgifter i

1. dataskyddsförordningen, lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning och föreskrifter som meddelats med stöd av den lagen när det gäller kamerabevakning som omfattas av förordningen eller den lagen, eller
2. brottsdatalagen (2018:000) och föreskrifter som meddelats med stöd av den lagen när det gäller kamerabevakning som omfattas av den lagen.

Bestämmelser i första stycket 1 eller 2 tillämpas på motsvarande sätt i fråga om sanktionsavgifter och skadestånd vid överträdelse av

bestämmelserna i denna lag eller av beslut som meddelats med stöd av lagen.

Vid tillämpning av bestämmelser om sanktionsavgifter gäller för myndigheter den högre avgiftsnivå som föreskrivs i lagen med kompletterande bestämmelser till EU:s dataskyddsförordning respektive brottsdatalagen.

Överklagande m.m.

Överklagande

29 § Tillsynsmyndighetens beslut enligt denna lag får överklagas till allmän förvaltningsdomstol.

Beslut om tillstånd till kamerabevakning och om undantag från kravet på upplysning om kamerabevakning får överklagas även av den kommun där bevakningen ska ske och, om kamerabevakningen ska avse en arbetsplats, av en organisation som företräder arbetstagarna på arbetsplatsen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Föreskrifter

30 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om avgifter för ansökningar enligt denna lag.

---

1. Denna lag träder i kraft den 25 maj 2018.
2. Genom lagen upphävs kameraövervakningslagen (2013:460).
3. Tillstånd till kameraövervakning som har beslutats enligt den äldre lagen och som avser kamerabevakning som omfattas av kravet på tillstånd i den nya lagen gäller fortfarande. Övriga tillstånd som har beslutats enligt den äldre lagen gäller inte längre.
4. Undantag från upplysningsplikten som har beslutats enligt den äldre lagen gäller fortfarande.
5. Anmälningar som har gjorts enligt den äldre lagen gäller inte längre.
6. Ärenden som har inletts hos länsstyrelserna enligt den äldre lagen men ännu inte har avgjorts överlämnas till den myndighet som utövar tillsyn över kamerabevakning enligt den nya lagen.
7. Mål som har överklagats till annan förvaltningsrätt än Förvaltningsrätten i Stockholm eller till annan kammarrätt än Kammarrätten i Stockholm enligt den äldre lagen men ännu inte har avgjorts överlämnas till Förvaltningsrätten i Stockholm respektive Kammarrätten i Stockholm. Om ett mål har överklagats av en enskild, är den myndighet som utövar tillsyn över kamerabevakning enligt den nya lagen motpart.
8. Äldre föreskrifter om skadestånd gäller fortfarande för skada som har orsakats före ikraftträdandet.
9. Äldre föreskrifter gäller fortfarande för överträdelser som har skett före ikraftträdandet.

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

Härigenom föreskrivs i fråga om offentlighets- och sekretesslagen (2009:400)

dels att 32 kap. 3 § ska ha följande lydelse,

dels att rubriken närmast efter 32 kap. 2 § ska lyda ”Kamerabevakning”.

Nuvarande lydelse	*Föreslagen lydelse*
32 kap.	
3 §[3]	
Sekretess gäller för sådan uppgift om en enskilds personliga förhållanden som har inhämtats genom *kameraövervakning* som avses i *kameraövervakningslagen (2013:460)*, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men.	Sekretess gäller för sådan uppgift om en enskilds personliga förhållanden som har inhämtats genom *kamerabevakning* som avses i *kamerabevakningslagen (2018:000)*, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men.

Sekretessen enligt första stycket gäller hos en domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

---

1. Denna lag träder i kraft den 25 maj 2018.
2. Äldre föreskrifter gäller fortfarande för uppgift som har inhämtats före ikraftträdandet.

[3] Senaste lydelse 2013:461.

Förteckning över remissinstanserna

Remissvar har lämnats av Riksdagens ombudsmän, Göta hovrätt, Solna tingsrätt, Falu tingsrätt, Göteborgs tingsrätt, Kammarrätten i Göteborg, Kammarrätten i Stockholm, Kammarrätten i Sundsvall, Förvaltningsrätten i Stockholm, Förvaltningsrätten i Falun, Förvaltningsrätten i Jönköping, Förvaltningsrätten i Umeå, Arbetsdomstolen, Justitiekanslern, Domstolsverket, Polismyndigheten, Säkerhetspolisen, Åklagarmyndigheten, Ekobrottsmyndigheten, Säkerhets- och integritetsskyddsnämnden, Brottsförebyggande rådet, Datainspektionen, Myndigheten för samhällsskydd och beredskap, Kustbevakningen, Försvarsmakten, Försvarets materielverk, Totalförsvarets forskningsinstitut, Försvarets radioanstalt, Tullverket, Socialstyrelsen, Länsstyrelsen i Dalarnas län, Länsstyrelsen i Norrbottens län, Länsstyrelsen i Stockholms län, Länsstyrelsen i Skåne län Länsstyrelsen i Västra Götalands län, Länsstyrelsen i Östergötlands län, Konsumentverket, Statens skolinspektion, Universitets- och högskolerådet, Myndigheten för yrkeshögskolan, Luleå tekniska universitet, Sveriges lantbruksuniversitet, Jordbruksverket, Naturvårdsverket, Transportstyrelsen, Trafikverket, Skogsstyrelsen, Luftfartsverket, Sjöfartsverket, Lantmäteriet, Arbetsmiljöverket, Arbetsgivarverket, Utredningen om självkörande fordon på väg (N 2015:07), Jönköpings kommun, Karlskrona kommun, Kristinehamns kommun, Malmö kommun, Skurups kommun, Stockholms kommun Örnsköldsviks kommun, Stockholms läns landsting, Sveriges Kommuner och Landsting, Svenska Jägareförbund, Jägarnas Riksförbund, Sveriges advokatsamfund, SJ AB, Jernhusen AB, Sjöräddningssällskapet, Bildleverantörernas Förening, Svenska Journalistförbundet, Sveriges Television AB, Fastighetsägarna, Lantbrukarnas Riksförbund, Sveriges Jordägare, Riksidrottsförbundet, Postnord AB, Svensk Kollektivtrafik, Svenska bankföreningen, Hyresgästföreningen, Mäklarsamfundet, Skogsindustrierna, Sveriges byggindustrier, Visita, SWESEC (Svenska säkerhetsföretag), Svensk Handel, Svenskt Näringsliv, Almega, Tjänstemännens Centralorganisation (TCO), Sveriges Akademikers Centralorganisation (SACO) och Landsorganisationen i Sverige (LO).

Universitetskanslerämbetet, Stockholms universitet, Arvika kommun, Askersunds kommun, Bräcke kommun, Dorotea kommun, Eksjö kommun, Falu kommun, Kiruna kommun, Mariestads kommun, Munkedals kommun, Nacka kommun, Nordmalings kommun, Oskarshamns kommun, Skellefteå kommun, Strömstads kommun, Sundsvall kommun, Trollhättans kommun, Uddevalla kommun, Vansbro kommun, Vimmerby kommun, Värmdö kommun, Västerås kommun, Ängelholms kommun, Skåne läns landsting, Östergötlands läns landsting, Västra Götalands läns landsting, Värmlands läns landsting, Jämtlands läns landsting, TU Medier i Sverige, Utgivarna, Swedavia AB, Missing People Sweden och Civil Rights Defenders har avstått från att lämna synpunkter på förslagen i betänkandet eller har inte svarat på remissen.

Synpunkter har också lämnats av Länsstyrelsen Gävleborg, Länsstyrelsen i Uppsala län, Aktiebolaget Östgötatrafiken, Säkerhetsbranschen, Säkerhet för Näringsliv & Samhälle (SNOS),

Svenska rovdjursföreningen, Sveriges Bussföretag, Säkerhetsföretagen, specialiståklagaren Christer B. Jarlås (Riksenheten för miljö- och arbetsmiljömål), Världsnaturfonden, BIL Sweden, Scientific engineering QED, Insamlingsstiftelsen APU Sweden.

Bilaga 5