Svensk författningssamling

Brottsdatalag

SFS 2018:1177
Publicerad
den 27 juni 2018

Utfärdad den 20 juni 2018

Enligt riksdagens beslut[1] föreskrivs[2] följande.

1 kap. Allmänna bestämmelser

Syftet med lagen

1 § Genom denna lag genomförs 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 dataskyddsdirektivet.

Syftet med lagen är att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter och att säkerställa att behöriga myndigheter kan behandla och utbyta personuppgifter med varandra på ett ändamålsenligt sätt.

Lagens tillämpningsområde

2 § Denna lag gäller vid behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Den gäller också vid behandling av personuppgifter som en behörig myndighet utför i syfte att upprätthålla allmän ordning och säkerhet.

3 § Lagen gäller vid sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

4 § Lagen gäller inte vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet eller om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen.

Lagen gäller inte heller i sådan verksamhet som omfattas av lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

[1] Prop. 2017/18:232, bet. 2017/18:JuU37, rskr. 2017/18:392.
[2] 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.

5 § Om en annan lag eller en förordning innehåller någon bestämmelse som avviker från denna lag, tillämpas den bestämmelsen.

Definitioner

6 § I denna lag används följande uttryck med nedan angiven betydelse.

Uttryck	*Betydelse*
Behandling av personuppgifter	En åtgärd eller kombination av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter, oavsett om det görs automatiserat eller inte, t.ex. insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande, spridning eller tillhandahållande på annat sätt, justering, sammanföring, begränsning, radering eller förstöring.
Behörig myndighet	1. En myndighet som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder, eller upprätthålla allmän ordning och säkerhet, när den behandlar personuppgifter för ett sådant syfte, eller 2. en annan aktör som har anförtrotts myndighetsutövning för ett syfte som anges i 1, när den behandlar personuppgifter för ett sådant syfte.
Biometriska uppgifter	Personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen.
Dataskyddsombud	Den som utses av den personuppgiftsansvarige för att självständigt kontrollera att personuppgifter behandlas författningsenligt och på ett korrekt sätt enligt vad som närmare anges i lagen.
Genetiska uppgifter	Personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som härrör från analys av ett spår av eller ett prov från personen.
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 stater.
Medlemsstat	En stat som är medlem i Europeiska unionen samt Island, Liechtenstein, Norge och Schweiz.

Mottagare	Den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision.
Personuppgift	Varje upplysning om en identifierad eller identifierbar fysisk person som är i livet.
Personuppgiftsansvarig	Den behöriga myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.
Personuppgiftsbiträde	Den som behandlar personuppgifter för den personuppgiftsansvariges räkning.
Personuppgiftsincident	En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt röjande av eller obehörig åtkomst till personuppgifter.
Registrerad	Den fysiska person som personuppgiften gäller.
Tillsynsmyndigheten	Myndighet som regeringen utser enligt dataskyddsdirektivet för att utöva tillsyn över behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.
Tredjeland	En stat som inte är en medlemsstat.
Tredje man	Någon annan än den registrerade, den personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar har rätt att behandla personuppgifter.
Uppgift som rör hälsa	Personuppgift som rör en persons fysiska eller psykiska hälsa, inklusive information om tillhandahållande av hälso- och sjukvårdstjänster som ger upplysning om personens hälsostatus.

2 kap. Behandling av personuppgifter

Grundläggande krav på behandlingen

Rättsliga grunder

1 § Personuppgifter får behandlas om det är nödvändigt för att en behörig myndighet ska kunna utföra sin uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.

Med en behörig myndighets uppgift avses en uppgift som framgår av lag, förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att utföra uppgiften.

2 § Utöver vad som sägs i 1 § får personuppgifter behandlas om

1. det är nödvändigt för diarieföring, eller

2. uppgifterna har lämnats till en behörig myndighet i en anmälan, ansökan eller liknande och behandlingen är nödvändig för myndighetens handläggning.

Ändamål

3 § Personuppgifter får behandlas bara för särskilda, uttryckligt angivna och berättigade ändamål.

Om det ändamål som personuppgifterna behandlas för inte framgår av sammanhanget eller på annat sätt, ska det tydliggöras genom en särskild upplysning.

4 § Innan personuppgifter får behandlas för ett nytt ändamål ska det säkerställas att

1. det finns en rättslig grund enligt 1 § för den nya behandlingen, och

2. det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet.

I den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning ska någon prövning enligt första stycket inte göras.

5 § En behörig myndighet får behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom denna lags tillämpningsområde.

Författningsenlig och korrekt behandling

6 § Personuppgifter ska behandlas författningsenligt och på ett korrekt sätt.

Personuppgifternas kvalitet

7 § Personuppgifter som behandlas ska vara korrekta och, om det är nödvändigt, uppdaterade.

Uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet.

8 § Personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Åtskillnad mellan olika slag av personuppgifter

9 § Så långt det är möjligt ska personuppgifter som rör olika kategorier av registrerade särskiljas så att det framgår om personen är misstänkt, dömd för brott, brottsoffer eller någon annan som berörs av ett brott. Om det inte framgår av sammanhanget eller på annat sätt till vilken kategori personen hör, ska det tydliggöras genom en särskild upplysning.

10 § Så långt det är möjligt ska personuppgifter som grundar sig på fakta särskiljas från personuppgifter som grundar sig på personliga bedömningar. Om det inte framgår av sammanhanget eller på annat sätt vad uppgiften grundas på ska det tydliggöras genom en särskild upplysning.

11 § Personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning får inte behandlas.

Om uppgifter om en person behandlas får de dock kompletteras med sådana uppgifter som anges i första stycket när det är absolut nödvändigt för ändamålet med behandlingen.

12 § Biometriska uppgifter och genetiska uppgifter får behandlas endast om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen.

13 § Personuppgifter som avses i 11 och 12 §§ (känsliga personuppgifter) får alltid behandlas med stöd av 2 §.

14 § Det är förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter.

Rättelse, uppdatering och radering

15 § Alla rimliga åtgärder ska vidtas för att personuppgifter som med hänsyn till ändamålet med behandlingen är felaktiga eller ofullständiga utan onödigt dröjsmål rättas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Personuppgifter som är inaktuella ska uppdateras om det är nödvändigt.

När personuppgifter lämnas ut till en behörig myndighet ska mottagaren så långt det är möjligt ges information som gör att det går att bedöma i vilken utsträckning uppgifterna är korrekta, fullständiga, uppdaterade och tillförlitliga.

16 § Alla rimliga åtgärder ska vidtas för att personuppgifter som behandlas i strid med 1, 2, 3 § första stycket eller någon av 4–6 §§ eller 8, 11, 12, 14 eller 17 § första stycket utan onödigt dröjsmål raderas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Detsamma gäller om radering krävs för att utföra en rättslig förpliktelse.

Om förutsättningarna i första stycket för att radera personuppgifter är uppfyllda men uppgifterna behöver finnas kvar av bevisskäl, ska behandlingen av uppgifterna i stället utan onödigt dröjsmål begränsas.

Längsta tid som personuppgifter får behandlas

17 § Personuppgifter får inte behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

Bestämmelsen i första stycket hindrar inte att en behörig myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet.

18 § Om det inte är föreskrivet i lag eller annan författning när en viss kategori av personuppgifter inte längre får behandlas för ändamål inom denna lags tillämpningsområde, ska den personuppgiftsansvarige årligen se över behovet av att fortsätta behandla personuppgifterna.

19 § Om ett beslut har rättsliga följder för en fysisk person eller annars i betydande grad påverkar honom eller henne och beslutet enbart grundas på automatiserad behandling av sådana personuppgifter som är avsedda att bedöma hans eller hennes egenskaper, ska personen ha möjlighet att på begäran få beslutet prövat på nytt av någon person.

Automatiserade beslut får inte enbart grundas på känsliga personuppgifter.

Överföring av personuppgifter till en annan medlemsstat

20 § Om det inte är särskilt föreskrivet får villkor för behandling av personuppgifter inte ställas upp i förhållande till en mottagare i en annan medlemsstat eller ett EU-organ, om det inte i motsvarande fall får ställas upp samma typ av villkor i förhållande till en svensk mottagare.

Uppgiftslämnande för rättsstatistik

21 § Personuppgifter som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

Behandling för ändamål utanför denna lags tillämpningsområde

22 § Innan personuppgifter som behandlas med stöd av denna lag behandlas för ett ändamål utanför lagens tillämpningsområde ska det säkerställas att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det ändamålet.

I den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning ska någon prövning enligt första stycket inte göras.

3 kap. Personuppgiftsansvarigas skyldigheter

Personuppgiftsansvarets omfattning

1 § Den personuppgiftsansvarige är ansvarig för all behandling av personuppgifter som utförs under dennes ledning eller på dennes vägnar.

Åtgärder för att säkerställa författningsenlig behandling

Tekniska och organisatoriska åtgärder

2 § Den personuppgiftsansvarige ska, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att den registrerades rättigheter skyddas.

3 § Den personuppgiftsansvarige ska när medlen för behandlingen bestäms och vid behandlingen, genom lämpliga tekniska och organisatoriska åtgärder, se till att nödvändiga skyddsåtgärder integreras i behandlingen (inbyggt dataskydd).

4 § Den personuppgiftsansvarige ska se till att det i automatiserade behandlingssystem som regel inte är möjligt att behandla andra personuppgifter än de som är nödvändiga för varje särskilt angivet ändamål med behandlingen (dataskydd som standard).

5 § Den personuppgiftsansvarige ska säkerställa att det i automatiserade behandlingssystem förs loggar över personuppgiftsbehandling i den utsträckning det är särskilt föreskrivet.

6 § Den personuppgiftsansvarige ska se till att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Konsekvensbedömning och förhandssamråd

7 § Om en ny typ av behandling, eller betydande förändringar av redan pågående behandling, kan antas medföra särskild risk för intrång i den registrerades personliga integritet, ska den personuppgiftsansvarige 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 samråda med tillsynsmyndigheten i god tid innan behandlingen påbörjas eller betydande förändringar genomförs (förhandssamråd).

Säkerheten för personuppgifter

Säkerhetsåtgärder

8 § Den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada.

Personuppgiftsincidenter

9 § Senast 72 timmar efter det att den personuppgiftsansvarige fått kännedom om en personuppgiftsincident ska den anmälas till tillsynsmyndigheten, utom i de fall där incidenten ska rapporteras enligt säkerhetsskyddslagen (1996:627) eller föreskrifter som har meddelats i anslutning till den lagen.

Anmälan behöver inte göras om det är osannolikt att personuppgiftsincidenten har medfört eller kommer att medföra någon risk för otillbörligt intrång i registrerades personliga integritet.

10 § Om en personuppgiftsincident som ska anmälas enligt 9 § första stycket har medfört eller kan antas medföra särskild risk för otillbörligt intrång i registrerades personliga integritet, ska den personuppgiftsansvarige utan onödigt dröjsmål underrätta den registrerade om incidenten.

Underrättelseskyldigheten gäller inte om den personuppgiftsansvarige

1. har tillämpat lämpliga tekniska och organisatoriska skyddsåtgärder på de personuppgifter som påverkades av incidenten,
2. har säkerställt att det inte längre finns särskild risk för otillbörligt intrång i registrerades personliga integritet, eller
3. skulle behöva göra oproportionerliga ansträngningar för att underrätta alla berörda.

I fall som avses i andra stycket 3 ska allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade får nödvändig information.

11 § Den personuppgiftsansvarige får avstå från att lämna information enligt 10 § 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 intresset av att

1. förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,

2. andra rättsliga utredningar eller undersökningar inte hindras,

3. nationell säkerhet skyddas, eller

4. någon annans rättigheter och friheter skyddas.

Om den personuppgiftsansvarige inte är en myndighet, gäller undantaget i första stycket även för uppgifter som hos en myndighet skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen (2009:400).

Samarbete med tillsynsmyndigheten

12 § Den personuppgiftsansvarige ska samarbeta med tillsynsmyndigheten när den utför uppgifter enligt denna lag och föreskrifter som har meddelats i anslutning till lagen.

Dataskyddsombud

13 § Den personuppgiftsansvarige ska utse ett eller flera dataskyddsombud och anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

14 § Dataskyddsombud ska

1. självständigt kontrollera att den personuppgiftsansvarige behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör sina skyldigheter,

2. informera och ge råd till den personuppgiftsansvarige och de som behandlar personuppgifter under dennes ledning om deras skyldigheter vid behandling av personuppgifter,

3. på begäran ge den personuppgiftsansvarige råd vid en konsekvensbedömning och kontrollera att den genomförs på korrekt sätt,

4. vara kontaktpunkt för enskilda i frågor som rör behandling av personuppgifter, och

5. samarbeta med tillsynsmyndigheten och vara kontaktpunkt för den vid förhandssamråd och andra frågor som rör behandling av personuppgifter.

15 § Den som fullgör uppgift som dataskyddsombud får inte obehörigen röja det som han eller hon vid fullgörandet av sin uppgift har fått kännedom om.

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

Personuppgiftsbiträden

16 § Den personuppgiftsansvarige får, om det är lämpligt, anlita personuppgiftsbiträden för behandling av personuppgifter på den personuppgiftsansvariges vägnar. Innan ett personuppgiftsbiträde anlitas ska den personuppgiftsansvarige försäkra sig om att biträdet kommer att vidta de lämpliga tekniska och organisatoriska åtgärder som krävs för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda registrerades rättigheter.

Personuppgiftsbiträdets behandling av personuppgifter ska regleras i ett skriftligt avtal eller annan skriftlig överenskommelse.

17 § Ett personuppgiftsbiträde får inte anlita ett annat personuppgiftsbiträde utan skriftligt tillstånd från den personuppgiftsansvarige.

18 § Ett personuppgiftsbiträde och de som arbetar under biträdets ledning ska behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige.

Om ett personuppgiftsbiträde bestämmer ändamålen med och medlen för behandlingen, ska biträdet anses vara personuppgiftsansvarig för den behandlingen.

19 § Det som sägs om den personuppgiftsansvariges skyldigheter i 5, 6, 8 och 12 §§ gäller även för personuppgiftsbiträden.

Gemensamt personuppgiftsansvar

20 § Två eller flera behöriga myndigheter är gemensamt personuppgiftsansvariga om de gemensamt bestämmer ändamålen med och medlen för personuppgiftsbehandlingen.

Den registrerade får utöva sina rättigheter enligt lagen mot var och en av de gemensamt personuppgiftsansvariga.

Bemyndigande

21 § Regeringen får meddela föreskrifter om skyldighet att föra register över kategorier av behandling av personuppgifter och skyldighet att införa interna rutiner för anmälan av överträdelser.

4 kap. Enskildas rättigheter

Rätten till information

Allmän information

1 § Den personuppgiftsansvarige ska göra följande allmänna information tillgänglig för den registrerade:

1. den personuppgiftsansvariges identitet och kontaktuppgifter,
2. dataskyddsombudets kontaktuppgifter,
3. kategorier av ändamål för behandlingen,
4. rätten enligt 3 § att begära att få information om behandling av personuppgifter och att få del av uppgifterna,
5. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 9 och 10 §§, och
6. möjligheten att lämna in klagomål till tillsynsmyndigheten samt kontaktuppgifterna till myndigheten.

Personrelaterad information

2 § Den personuppgiftsansvarige ska i ett enskilt fall lämna följande information till den registrerade, om det behövs för att han eller hon ska kunna ta till vara sina rättigheter:

1. den rättsliga grunden för behandlingen,
2. kategorier av mottagare av personuppgifterna, även i tredjeland eller internationella organisationer,
3. hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det, och
4. övrig nödvändig information.

Vid bedömningen av om information enligt första stycket 4 ska lämnas ska det särskilt beaktas om personuppgifterna samlats in utan den registrerades vetskap.

3 § Den personuppgiftsansvarige ska till den som begär det utan onödigt dröjsmål lämna skriftligt besked om huruvida personuppgifter som rör honom eller henne behandlas. Om sådana uppgifter behandlas, ska sökanden få del av dem och få följande skriftliga information:

1. vilka personuppgifter om sökanden som behandlas,
2. varifrån personuppgifterna kommer,
3. den rättsliga grunden för behandlingen,
4. ändamålen med behandlingen,
5. mottagare eller kategorier av mottagare av personuppgifterna, även i tredjeland eller internationella organisationer,
6. hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det,
7. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 9 och 10 §§, och
8. möjligheten att lämna in klagomål till tillsynsmyndigheten samt kontaktuppgifterna till myndigheten.

Utlämnande av personuppgifter enligt första stycket behöver inte omfatta sådana personuppgifter som sökanden har tagit del av, om inte han eller hon begär det. Det ska dock framgå av informationen att personuppgifterna i fråga behandlas.

4 § Den som har varit föremål för ett sådant beslut som avses i 2 kap. 19 § har rätt att på begäran få närmare information om beslutet av den personuppgiftsansvarige.

Begränsning av rätten till information

5 § Informationsskyldigheten i 2 och 3 §§ gäller 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 intresset av att

1. förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,
2. andra rättsliga utredningar eller undersökningar inte hindras,
3. nationell säkerhet skyddas, eller
4. någon annans rättigheter och friheter skyddas.

Om förutsättningarna i första stycket är uppfyllda, är den personuppgiftsansvarige inte skyldig att lämna ut skälen för beslut enligt första stycket eller beslut i fråga om rättelse, radering eller begränsning av behandlingen enligt 9 eller 10 §.

Om den personuppgiftsansvarige inte är en myndighet, gäller undantagen i första och andra styckena även för uppgifter som hos en myndighet skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen (2009:400).

6 § Informationsskyldigheten i 3 § gäller inte personuppgifter i löpande text som inte har fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande.

Informationsskyldigheten gäller dock om uppgifterna

1. har lämnats ut till tredje man, med undantag för en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision,
2. behandlas enbart för vetenskapliga, statistiska eller historiska ändamål, eller

3. har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

7 § Om en begäran enligt 3 § är orimlig eller uppenbart ogrundad får den personuppgiftsansvarige avslå den.

Av 12 § andra stycket framgår att den personuppgiftsansvarige i vissa fall får ta ut avgift i stället för att avslå begäran.

Möjligheten att begära kontroll genom tillsynsmyndigheten

8 § I 5 kap. 3 § finns bestämmelser om att en fysisk person får begära att tillsynsmyndigheten kontrollerar om hans eller hennes personuppgifter behandlas författningsenligt.

Rätten till rättelse, radering och begränsning av behandlingen

9 § Den personuppgiftsansvarige ska på begäran av den registrerade utan onödigt dröjsmål rätta eller komplettera personuppgifter som rör honom eller henne, om de är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen.

Om den personuppgiftsansvarige inte kan fastställa att personuppgifterna är korrekta ska behandlingen av uppgifterna i stället utan onödigt dröjsmål begränsas.

10 § Den personuppgiftsansvarige ska på begäran av den registrerade utan onödigt dröjsmål radera personuppgifter som rör honom eller henne, om de behandlas i strid med 2 kap. 1, 2, 3 § första stycket eller någon av 4–6 §§ eller 8, 11, 12, 14 eller 17 § första stycket. Detsamma gäller om det krävs radering för att den personuppgiftsansvarige ska utföra en rättslig förpliktelse.

Om förutsättningarna i första stycket för att radera personuppgifter är uppfyllda men uppgifterna behöver finnas kvar av bevisskäl, ska den personuppgiftsansvarige på begäran av den registrerade i stället utan onödigt dröjsmål begränsa behandlingen av uppgifterna.

11 § Den personuppgiftsansvarige avgör vilken åtgärd som ska vidtas med anledning av en begäran om rättelse, radering eller begränsning av behandlingen.

Avgiftsfri information

12 § Information enligt 1, 2 och 4 §§ ska lämnas utan avgift. Information och uppgifter enligt 3 § ska lämnas utan avgift en gång per år.

Om någon begär information och uppgifter enligt 3 § oftare än en gång per år, får den personuppgiftsansvarige ta ut en rimlig avgift eller avslå begäran enligt 7 § första stycket.

5 kap. Tillsyn

Tillsynsmyndighetens uppdrag

1 § Tillsynsmyndigheten ska verka både för att fysiska personers grundläggande rättigheter och friheter skyddas i samband med behandling av personuppgifter och för att underlätta det fria flödet av personuppgifter inom denna lags tillämpningsområde.

2 § Tillsynsmyndigheten ska
1. utöva allmän tillsyn över personuppgiftsbehandling,
2. handlägga klagomål från registrerade,
3. utföra kontroll enligt 3 §, och
4. på begäran bistå en tillsynsmyndighet i en annan medlemsstat.

Tillsynen ska inte omfatta behandling av personuppgifter inom ramen för domstolarnas dömande verksamhet.

3 § Tillsynsmyndigheten ska på begäran kontrollera om uppgifter om en fysisk person behandlas författningsenligt. Den som begär en sådan kontroll ska visa att han eller hon har begärt information enligt 4 kap. 3 § eller en åtgärd enligt 4 kap. 9 eller 10 §.

Myndigheten får vägra att utföra kontrollen om begäran är orimlig eller uppenbart ogrundad.

4 § Tillsynsmyndigheten ska vid förhandssamråd enligt 3 kap. 7 § och när det i övrigt är påkallat ge råd och stöd till personuppgiftsansvariga och personuppgiftsbiträden om deras skyldigheter enligt lag eller annan författning.

Tillsynsmyndighetens befogenheter

Undersökningsbefogenheter

5 § Tillsynsmyndigheten har rätt att av personuppgiftsansvariga och personuppgiftsbiträden på begäran få
1. tillgång till alla personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder,
3. tillträde till lokaler som den personuppgiftsansvarige eller personuppgiftsbiträdet disponerar samt tillgång till utrustning och andra medel för behandling av personuppgifter, och
4. den hjälp och den information som behövs för tillsynen.

Förebyggande befogenheter

6 § Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska myndigheten genom råd, rekommendationer eller påpekanden försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att motverka den risken.

Tillsynsmyndigheten får utfärda en skriftlig varning för att planerad behandling av personuppgifter riskerar att stå i strid med lag eller annan författning. Detsamma gäller om pågående behandling riskerar att stå i strid med lag eller annan författning.

Korrigerande befogenheter

7 § Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning eller att den personuppgiftsansvarige eller personuppgiftsbiträdet på något annat sätt inte fullgör sina skyldigheter, får tillsynsmyndigheten
1. genom sådana åtgärder som anges i 6 § första stycket försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig, eller att uppfylla andra skyldigheter,

2. förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter,

3. förbjuda fortsatt behandling om bristen är allvarlig, eller

4. besluta om en sanktionsavgift enligt 6 kap.

Om ett föreläggande utfärdas ska det av föreläggandet framgå när åtgärderna senast ska vara genomförda och, om det är lämpligt, vilka åtgärder som ska vidtas.

Verkställighet av beslut

8 § Tillsynsmyndighetens beslut får inte verkställas omedelbart.

Samarbete med tillsynsmyndigheter i andra medlemsstater

9 § Tillsynsmyndigheten får vägra en begäran om bistånd från en tillsynsmyndighet i en annan medlemsstat endast om det skulle strida mot en lag eller en förordning att tillmötesgå den.

10 § När tillsynsmyndigheten på begäran bistår en tillsynsmyndighet i en annan medlemsstat har den de befogenheter som anges i 5–7 §§.

11 § Tillsynsmyndigheten får, om det är förenligt med svenska intressen, lämna ut en uppgift till en tillsynsmyndighet i en annan medlemsstat, även om uppgiften är sekretessbelagd enligt offentlighets- och sekretesslagen (2009:400).

12 § Information som tillsynsmyndigheten efter begäran har fått från en tillsynsmyndighet i en annan medlemsstat får inte användas för något annat ändamål än det för vilket informationen begärdes.

6 kap. Administrativa sanktionsavgifter

Överträdelser som kan leda till en sanktionsavgift

1 § En sanktionsavgift får tas ut av en personuppgiftsansvarig vid överträdelse av någon av

1. 2 kap. 1–5, 7–12 eller 14–18 §§, 19 § andra stycket eller 22 §,
2. 3 kap. 2–8 §§, eller
3. 8 kap. 1–6 §§ eller 8 §.

En sanktionsavgift får också tas ut om en personuppgiftsansvarig inte anmäler en personuppgiftsincident enligt 3 kap. 9 § första stycket, inte dokumenterar en sådan incident, låter bli att bistå tillsynsmyndigheten enligt 5 kap. 5 § eller inte följer tillsynsmyndighetens beslut enligt 5 kap. 7 § första stycket 2 eller 3.

2 § En sanktionsavgift får tas ut av ett personuppgiftsbiträde vid överträdelse av 3 kap. 5, 6 eller 8 §.

En sanktionsavgift får också tas ut om ett personuppgiftsbiträde låter bli att bistå tillsynsmyndigheten enligt 5 kap. 5 § eller inte följer tillsynsmyndighetens beslut enligt 5 kap. 7 § första stycket 2 eller 3.

Hur sanktionsavgiften ska bestämmas

3 § Sanktionsavgiften ska vid överträdelser av 3 kap. 6 eller 7 § eller av bestämmelser om dokumentation av personuppgiftsincidenter bestämmas till högst 5 000 000 kronor.

Vid överträdelser av övriga bestämmelser som anges i 1 och 2 §§ ska avgiften bestämmas till högst 10 000 000 kronor.

Om flera bestämmelser har överträtts genom samma personuppgiftsbehandling, eller om en eller flera bestämmelser har överträtts genom sammankopplade personuppgiftsbehandlingar, ska sanktionsavgiften bestämmas efter överträdelsernas allvar. Sanktionsavgiften får aldrig överstiga maximibeloppet för den allvarligaste överträdelsen.

4 § Vid bedömningen av om någon sanktionsavgift ska tas ut och när storleken på avgiften ska bestämmas ska särskild hänsyn tas till

1. om överträdelsen varit uppsåtlig eller berott på oaktsamhet,
2. den skada, fara eller kränkning som överträdelsen inneburit,
3. överträdelsens karaktär, svårhetsgrad och varaktighet,
4. vad den personuppgiftsansvarige eller personuppgiftsbiträdet gjort för att begränsa verkningarna av överträdelsen, och
5. om den personuppgiftsansvarige eller personuppgiftsbiträdet tidigare ålagts att betala en sanktionsavgift.

5 § Sanktionsavgiften får sättas ned helt eller delvis om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut en avgift.

Beslut om sanktionsavgift

6 § Tillsynsmyndigheten beslutar om sanktionsavgift.

Sanktionsavgiften tillfaller staten.

7 § En sanktionsavgift får inte beslutas om den som avgiften ska tas ut av inte har fått tillfälle att yttra sig inom fem år från den dag då överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

Betalning av sanktionsavgift

8 § En sanktionsavgift ska betalas till den myndighet som regeringen bestämmer inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom den tid som anges i första stycket, ska myndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

Bemyndigande

9 § Regeringen får meddela ytterligare föreskrifter om sanktionsavgifter enligt denna lag.

7 kap. Skadestånd och överklagande

Skadestånd

1 § Den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som orsakats av behandling av personuppgifter i strid med denna lag, eller föreskrifter som har meddelats i anslutning till den.

Överklagande av personuppgiftsansvariga myndigheters beslut

2 § Beslut i fråga om rättelse eller komplettering enligt 4 kap. 9 § första stycket, radering enligt 4 kap. 10 § första stycket, eller begränsning av behandlingen enligt 4 kap. 9 § andra stycket eller 10 § andra stycket, som har meddelats av en myndighet i egenskap av personuppgiftsansvarig, får överklagas till allmän förvaltningsdomstol. Detsamma gäller beslut att inte lämna information enligt 4 kap. 3 §, att ta ut avgift enligt 4 kap. 12 § andra stycket eller att inte medge prövning av ett automatiserat beslut enligt 2 kap. 19 § första stycket.

Prövningstillstånd krävs vid överklagande till kammarrätten.

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

Överklagande av tillsynsmyndighetens beslut

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

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagandeförbud

4 § Andra beslut enligt denna lag än de som avses i 2 och 3 §§ får inte överklagas.

8 kap. Överföring av personuppgifter till tredjeland och internationella organisationer

Förutsättningar för överföring

1 § En behörig myndighet får överföra personuppgifter till ett tredjeland eller en internationell organisation, om personuppgifterna behandlas i Sverige eller är avsedda att behandlas i ett tredjeland eller av en internationell organisation. Personuppgifterna får dock endast överföras om överföringen

1. är nödvändig för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,
2. riktas till en behörig myndighet i ett tredjeland eller till en internationell organisation som är en behörig myndighet, och
3. omfattas av

a) ett beslut om adekvat skyddsnivå enligt 3 §,

b) tillräckliga skyddsåtgärder enligt 4 §, eller

c) ett undantag för särskilda situationer enligt 5 §.

En behörig myndighet som avser att överföra personuppgifter till ett tredjeland eller en internationell organisation, ska särskilt beakta risken för att enskilda får ett försämrat skydd för sina personuppgifter.

2 § Personuppgifter som en svensk myndighet har fått från en annan medlemsstat får överföras till ett tredjeland eller en internationell organisation endast om den medlemsstat som lämnat uppgifterna till en svensk myndighet har medgett att de överförs.

Om medgivandet på grund av tidsbrist inte kan inhämtas i förväg, får personuppgifter ändå överföras om det är nödvändigt för att avvärja en omedelbar och allvarlig fara för allmän säkerhet. Detsamma gäller om det

är nödvändigt för att avvärja en omedelbar och allvarlig fara för andra väsentliga intressen för Sverige eller någon annan medlemsstat.

Beslut om adekvat skyddsnivå

3 § Om Europeiska kommissionen har beslutat att det finns en adekvat nivå för skyddet av personuppgifter i ett tredjeland, eller en viss geografisk eller på annat sätt angiven del av det, får personuppgifter överföras dit under de förutsättningar som anges i 1 och 2 §§. Detsamma gäller om det finns ett sådant beslut avseende en internationell organisation.

Tillräckliga skyddsåtgärder

4 § Om det inte finns något beslut om adekvat skyddsnivå enligt 3 §, får personuppgifter, under de förutsättningar som anges i 1 och 2 §§, ändå överföras till ett tredjeland eller en internationell organisation om

1. skyddsåtgärder för personuppgifterna har fastställts i ett avtal som ger tillräckliga garantier till skydd för den registrerade, eller
2. den behöriga myndighet som uppgifterna ska överföras till på annat sätt garanterar tillräckligt skydd för dem.

Överföring i särskilda situationer

5 § Om det inte finns något beslut om adekvat skyddsnivå enligt 3 § eller tillräckliga skyddsåtgärder enligt 4 §, får en överföring, eller en samling av överföringar, av personuppgifter, under de förutsättningar som anges i 1 och 2 §§, göras till ett tredjeland eller en internationell organisation endast om överföringen är nödvändig för att

1. värna den registrerades eller någon annan fysisk persons vitala intressen, eller andra berättigade intressen som den registrerade har,
2. i ett enskilt fall förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,
3. i ett enskilt fall kunna fastställa, göra gällande eller försvara ett rättsligt anspråk som hänför sig till ett sådant syfte som anges i 2, eller
4. avvärja en omedelbar och allvarlig fara för allmän säkerhet.

Personuppgifter får inte överföras till ett tredjeland eller en internationell organisation om den registrerades intresse av skydd mot kränkning av rättigheter och friheter väger tyngre än det allmännas intresse av en sådan överföring som avses i första stycket 2 eller 3.

Vidareöverföring

6 § En svensk behörig myndighet får inte tillåta att sådana personuppgifter som anges i 2 § första stycket, och som överförts till ett tredjeland eller en internationell organisation, vidareöverförs till ett tredjeland eller en internationell organisation, om inte någon behörig myndighet i den andra medlemsstaten har medgett att uppgifterna får vidareöverföras.

7 § När en svensk behörig myndighet ska ta ställning till om personuppgifter som har överförts från Sverige till en annan medlemsstat, som har överfört dem till ett tredjeland eller en internationell organisation, får vidareöverföras till ett tredjeland eller en internationell organisation, ska alla kända omständigheter som har samband med vidareöverföringen beaktas. Särskild vikt ska läggas vid brottets allvar, allvaret i faran för allmän säkerhet, det ändamål för vilket personuppgifterna ursprungligen lämnades till

den andra medlemsstaten och nivån på skyddet av personuppgifter i tredjelandet eller hos den internationella organisationen som uppgifterna ska vidareöverföras till.

Överföring till andra än behöriga myndigheter

8 § En svensk behörig myndighet får i ett enskilt fall överföra personuppgifter till någon som inte är en behörig myndighet i ett tredjeland. Personuppgifterna får överföras endast om de övriga förutsättningarna i 1 och 2 §§ är uppfyllda och om

1. det är absolut nödvändigt för att den svenska myndigheten ska kunna utföra en uppgift enligt 1 kap. 2 § som den har ansvar för,
2. den svenska myndigheten informerar den som ska ta emot personuppgifterna om det eller de specifika ändamål för vilket eller vilka uppgifterna får behandlas, och
3. det skulle vara ineffektivt eller olämpligt att överföra dem till en behörig myndighet i tredjelandet.

Personuppgifter får inte överföras enligt första stycket om den registrerades intresse av skydd mot kränkning av rättigheter och friheter väger tyngre än det allmännas intresse av att överföringen görs.

Första och andra styckena gäller inte en sådan annan aktör som är behörig myndighet enligt definitionen i 1 kap. 6 §.

Villkor om användningsbegränsning

9 § Om en svensk behörig myndighet har fått personuppgifter från ett tredjeland eller en internationell organisation och gäller på grund av en överenskommelse med tredjelandet eller den internationella organisationen villkor som begränsar möjligheten att använda uppgifterna, ska svenska myndigheter följa villkoren oavsett vad som är föreskrivet i lag eller annan författning.

10 § En svensk behörig myndighet får vid överföring av personuppgifter till ett tredjeland eller en internationell organisation i ett enskilt fall ställa upp villkor som begränsar möjligheten att använda uppgifterna, om det krävs med hänsyn till den enskildes rätt eller från allmän synpunkt. Sådana villkor får inte strida mot en internationell överenskommelse som är bindande för Sverige.

---

1. Denna lag träder i kraft den 1 augusti 2018.
2. Genom lagen upphävs lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen.
3. Bestämmelsen i 3 kap. 5 § om loggning tillämpas från och med den 6 maj 2023 i fråga om automatiserade behandlingssystem som inrättats före den 6 maj 2016.
4. En sanktionsavgift enligt 6 kap. får beslutas endast för överträdelser som har skett efter ikraftträdandet.
5. Äldre föreskrifter gäller fortfarande för överträdelser som har skett före ikraftträdandet.
6. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats före ikraftträdandet.

YLVA JOHANSSON

MORGAN JOHANSSON
(Justitiedepartementet)