Diarienummer
FK 2024/018853

Dataskydd och behandling av personuppgifter hos Försäkringskassan

En vägledning är i första hand ett stöd för Försäkringskassans medarbetare vid ärendehandläggning och utbildning. Den innehåller en samlad information om vad som gäller på det aktuella området, uppdelat på tillämpnings- och metodstödsavsnitt.

En vägledning kan innehålla beskrivningar av

- författningsbestämmelser
- allmänna råd
- förarbeten
- rättspraxis
- JO:s beslut.

En vägledning kan även innehålla beskrivningar av hur man ska handlägga ärenden på det aktuella området och vilka metoder som då ska användas.

Vägledningarna uppdateras fortlöpande. Ändringar arbetas in i den digitala versionen, som finns på forsakringskassan.se. Sök på ”vägledningar”.

Du som arbetar på Försäkringskassan hittar dem också på Fia.

Upplysningar: Försäkringskassan
Rättsavdelningen

Beslutad 2026-11-06

Innehåll

Förkortningar **7**

Begreppslista **8**

Sammanfattning **10**

Läsanvisningar **11**

1 När ska vi tillämpa bestämmelser om dataskydd? **12**
1.1 Reglering av rätt till skydd för den personliga integriteten 12
1.2 Dataskyddsförordningens tillämpningsområde 13
1.2.1 Vad är en personuppgift? 13
1.2.2 Vad är behandling av personuppgifter? 14
1.2.3 Behandling som sker helt eller delvis automatiskt 15
1.2.4 Behandling i register 15
1.2.5 Undantag från det materiella tillämpningsområdet 16
1.2.6 Territoriellt tillämpningsområde 17
1.3 Reglering som kompletterar dataskyddsförordningen 17
1.3.1 Tillämpningsområdet för 114 kap. SFB 18
1.3.2 Tillämpningsområdet för lagen om den officiella statistiken 19
1.3.3 Tillämpningsområdet för 7 kap. visselblåsarlagen 19

2 Roller och ansvar **21**
2.1 Personuppgiftsansvarig 21
2.2 Personuppgiftsbiträde 23
2.3 Dataskyddsombud 24

3 Grundläggande principer för behandling av personuppgifter **26**
3.1 Laglighet, korrekthet och öppenhet 26
3.2 Ändamålsbegränsning 27
3.3 Uppgiftsminimering 29
3.4 Riktighet 29
3.5 Lagringsminimering 31
3.6 Integritet och konfidentialitet 32
3.7 Ansvarsskyldighet 32

4 Rättslig grund **33**
4.1 Nödvändighetskravet 33
4.2 De rättsliga grunderna 34
4.2.1 Samtycke 34
4.2.2 Avtal 35
4.2.3 Rättslig förpliktelse 35
4.2.4 Uppgift av allmänt intresse eller led i myndighetsutövning 36
4.2.5 Intresseavvägning 37
4.3 Försäkringskassans kärnverksamhet 37
4.4 Särskilda statistikverksamheten 37
4.5 Visselblåsarlagen 37

5 Ändamål för behandling av personuppgifter **39**
5.1 Ändamål i kärnverksamheten 39
5.1.1 Tillgodose behov av underlag 39
5.1.2 Informera om förmåner och ersättningar 39

5.1.3 Handlägga ärenden ... 40
5.1.4 Vidta kontrollåtgärder ... 41
5.1.5 Verksamhetsplanering, resultatstyrning, resultatuppföljning, resultatredovisning, utvärdering eller tillsyn ... 42
5.1.6 Framställa statistik ... 42
5.1.7 Testverksamhet ... 43
5.1.8 Utlämnande av uppgifter ... 44
5.1.9 Behandling av personuppgifter med stöd av finalitetsprincipen ... 45
5.2 Ändamål i statistikverksamheten ... 45
5.3 Ändamål i visselblåsarlagen ... 46

6 Känsliga personuppgifter och andra särskilt skyddsvärda personuppgifter ... 48
6.1 Vad är känsliga personuppgifter? ... 48
6.2 När får känsliga personuppgifter behandlas? ... 50
6.3 Behandling med stöd av samtycke ... 50
6.4 Behandling inom arbetsrätten ... 51
6.5 Behandling vid rättsliga anspråk ... 52
6.6 Behandling av hänsyn till ett viktigt allmänt intresse ... 52
6.6.1 Behandling av känsliga personuppgifter i Försäkringskassans kärnverksamhet ... 54
6.6.2 Sökbegränsningar i Försäkringskassans kärnverksamhet ... 56
6.7 Behandling för arkiv-, forsknings- och statistikändamål ... 57
6.7.1 Arkivändamål ... 57
6.7.2 Statistikändamål ... 58
6.8 Behandling enligt visselblåsarlagen ... 59
6.9 Särskilt skyddsvärda personuppgifter ... 59
6.9.1 Personuppgifter om lagöverträdelser ... 59
6.9.2 Personnummer och samordningsnummer ... 60
6.9.3 Andra särskilt skyddsvärda personuppgifter ... 61

7 Dataskydd när personuppgifter lämnas ut från Försäkringskassan ... 62
7.1 Ett utlämnande av personuppgifter är en personuppgiftsbehandling ... 62
7.2 Utlämnande av personuppgifter i Försäkringskassans kärnverksamhet ... 64
7.3 Särskilt om utlämnande vid begäran om allmän handling ... 66
7.4 Säkerhetskrav gäller vid all behandling av personuppgifter ... 68

8 Tredjelandsöverföring ... 69
8.1 När är en tredjelandsöverföring tillåten? ... 69
8.1.1 Beslut om adekvat skyddsnivå ... 70
8.1.2 Lämpliga skyddsåtgärder ... 70
8.2 Undantag i särskilda situationer ... 72
8.3 Särskilt om extraterritoriell lagstiftning ... 72

9 Säkerhet vid personuppgiftsbehandling ... 73
9.1 Säkerhetsåtgärder ... 74
9.1.1 Pseudonymisering och kryptering ... 75
9.1.2 Tillgång till personuppgifter ... 76
9.1.3 Loggning ... 77
9.1.4 Inbyggt dataskydd och dataskydd som standard ... 78

10 Personuppgiftsbiträdesavtal ... 79
10.1 När behöver vi ett personuppgiftsbiträdesavtal? ... 79

10.2 Vad ska ett personuppgiftsbiträdesavtal innehålla? ... 80
10.2.1 Information om behandlingen, personuppgifterna, de registrerade och den personuppgiftsansvarigas skyldigheter och rättigheter ... 80
10.2.2 Dokumenterade instruktioner från den personuppgiftsansvariga ... 81
10.2.3 Konfidentialitet eller lagstadgad tystnadsplikt ... 82
10.2.4 Säkerhetsåtgärder ... 82
10.2.5 Underbiträden ... 83
10.2.6 De registrerades rättigheter ... 84
10.2.7 Bistå den personuppgiftsansvariga ... 84
10.2.8 När behandlingsuppdraget upphör ... 85
10.2.9 Tillgång till information, granskning och inspektioner ... 85
10.3 Standardavtalsklausuler ... 86

11 Rätten till information ... 88
11.1 Rätten till information när personuppgifter samlas in från den registrerade ... 88
11.1.1 Vad ska vi informera om? ... 88
11.1.2 Undantag från skyldigheten att informera ... 90
11.1.3 När ska vi informera? ... 91
11.1.4 Hur ska vi informera? ... 91
11.2 Rätten till information när vi inte fått personuppgifter från den registrerade ... 92
11.2.1 Vad ska vi informera om? ... 92
11.2.2 Undantag från skyldigheten att informera ... 94
11.2.3 När ska vi informera? ... 96
11.2.4 Hur ska vi informera? ... 96
11.3 Rätten till tillgång (registerutdrag) ... 97
11.3.1 Innehållet i ett registerutdrag ... 97
11.3.2 Personuppgifter som inte ska ingå i ett registerutdrag ... 100
11.3.3 När ska vi lämna ett registerutdrag? ... 101
11.3.4 Hur ska informationen i ett registerutdrag utformas? ... 102
11.3.5 Kostnad för registerutdrag ... 102
11.3.6 Avslagsbeslut ... 103

12 Övriga rättigheter ... 104
12.1 Rätten till rättelse ... 104
12.2 Rätten till radering ... 105
12.3 Rätten till begränsning ... 107
12.4 Rätten till dataportabilitet ... 108
12.5 Rätten att göra invändningar ... 109
12.6 Rätten att slippa automatiserat beslutsfattande, inbegripet profilering ... 109
12.7 Kostnad och beslut ... 111

13 Konsekvensbedömning ... 112
13.1 Vad ska vi bedöma? ... 112
13.2 När ska vi göra en konsekvensbedömning? ... 113
13.2.1 IMY:s förteckning ... 115
13.3 Vad en konsekvensbedömning ska innehålla ... 116
13.4 Inhämtande av synpunkter från registrerade ... 116
13.5 Undantag från kravet att göra en konsekvensbedömning ... 117
13.6 Förhandssamråd ... 117

14 Register över personuppgiftsbehandlingar 118
14.1 Register över personuppgiftsbehandlingar i egenskap av personuppgiftsansvarig 118
14.2 Register över personuppgiftsbehandlingar i egenskap av personuppgiftsbiträde 119

15 Personuppgiftsincidenter 120
15.1 När ska vi anmäla en personuppgiftsincident till IMY? 120
15.1.1 Bedöma risken vid en incident 121
15.1.2 Undantag från att anmäla en incident till IMY 122
15.2 När ska vi informera de registrerade? 122
15.3 Hur ska vi informera de registrerade? 123

16 Överklagande, tillsyn och skadestånd 124
16.1 Överklagande av beslut enligt dataskyddsförordningen 124
16.2 IMY:s tillsyn 124
16.2.1 Klagomål till IMY 124
16.2.2 Tillsyn 125
16.2.3 Vad tillsynen kan leda till 125
16.3 Skadestånd 128

Källförteckning 129

Förkortningar

Förkortning	Förklaring
Dataskyddslagen	Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning
EDPB	Europeiska dataskyddsstyrelsen
EU:s dataskyddsförordning eller dataskyddsförordningen	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)
Europakonventionen	Den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna
EU:s rättighetsstadga	Europeiska unionens stadga om de grundläggande rättigheterna (2010/C 83/02)
FL	Förvaltningslagen (2017:900)
Försäkringskassans instruktion	Förordningen (2009:1174) med instruktion för Försäkringskassan
HD	Högsta domstolen
HFD	Högsta förvaltningsdomstolen
IMY	Integritetsskyddsmyndigheten
JO	Justitieombudsmannen
JK	Justitiekanslern
KRNG	Kammarrätten i Göteborg
KRNJ	Kammarrätten i Jönköping
KRNS	Kammarrätten i Stockholm
KRSU	Kammarrätten i Sundsvall
NJA	Nytt Juridiskt Arkiv I (Domar från Högsta domstolen)
Prop.	Proposition
RF	Regeringsformen
RÅ	Regeringsrättens årsbok
OSL	Offentlighets- och sekretesslagen (2009:400)
SFB	Socialförsäkringsbalken
SOU	Statens offentliga utredningar
TF	Tryckfrihetsförordningen
Visselblåsarlagen	Lagen (2021:890) om skydd för personer som rapporterar missförhållanden
YGL	Yttrandefrihetsgrundlagen

Begreppslista

Det dataskyddsrättsliga området innehåller många begrepp som är viktiga att hålla reda på. I tabellen finns de vanligaste.

Begrepp	Förklaring	Rättslig definition i dataskydds-förordningen	Läs mer
Behandling av personuppgifter Personuppgiftsbehandling	I princip allt som kan göras med personuppgifter, till exempel insamling, registrering, organisering, strukturering, lagring, bearbetning, ändring, framtagning, sökning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, radering eller förstöring. En behandling kan vara antingen en enskild åtgärd eller en kombination av åtgärder som vidtas för samma ändamål.	Artikel 4.2	Avsnitt 1.2.2
Dataskyddsombud	Utnämns av en personuppgiftsansvarig eller ett personuppgiftsbiträde. Ombudet ska övervaka att dataskyddsreglerna följs, men har inget ansvar för att så sker. Ombudet ska också informera och ge råd samt vara kontaktpunkt för tillsynsmyndigheten och för registrerade personer.	Artikel 37–39	Avsnitt 2.3
Finalitetsprincipen	När personuppgifter har samlats in för ett visst ändamål, får de inte därefter behandlas för ett ändamål som är oförenligt med det ursprungliga ändamålet.	Artikel 5.1 b och 6.4	Avsnitt 3.2, 5.1.9 och 6.6.1
Försäkringskassans kärnverksamhet	Den verksamhet som handlar om att administrera socialförsäkringen och andra förmåner som Försäkringskassan enligt lag eller förordning ansvarar för (jämför 1 § Försäkringskassans instruktion).		
Kategori av personuppgifter	Övergripande indelning av olika typer av personuppgifter, till exempel kontaktuppgifter och ekonomiska uppgifter.		
Mottagare	En fysisk eller juridisk person som personuppgifter lämnas ut till. Det kan exempelvis vara ett personuppgiftsbiträde.	Artikel 4.9	
Personuppgift	Alla uppgifter som på något sätt kan knytas till en fysisk, levande person.	Artikel 4.1	Avsnitt 1.2.1
Personuppgift som är anonymiserad	En uppgift som tidigare har varit en personuppgift men som inte längre kan knytas till en fysisk person, varken ensam eller tillsammans med andra uppgifter. Uppgiften är därmed inte längre en personuppgift.	Skäl 26	Avsnitt 1.2.1
Personuppgift som är pseudonymiserad	En personuppgift, vars direkta koppling till en fysisk person har ersatts med ett löpnummer eller en annan identifikator. Uppgiften anses vara en personuppgift så länge den kan kopplas till en fysisk person genom att tillföra kompletterande uppgifter, till exempel en kodnyckel.	Artikel 4.5	Avsnitt 1.2.1
Personuppgift som är känslig (känsliga personuppgifter)	Vissa särskilda kategorier av personuppgifter, bland annat uppgifter om hälsa, uppgifter om en fysisk persons sexualliv eller sexuella läggning, genetiska uppgifter och uppgifter som avslöjar medlemskap i fackförening.	Artikel 9	Avsnitt 6.1

Begrepp	Förklaring	Rättslig definition i dataskydds-förordningen	Läs mer
Personuppgifter om lagöverträdelser	Vissa uppgifter om att en fysisk person misstänks för eller har begått ett brott.	Artikel 10	Avsnitt 6.9.1
Personuppgiftsansvarig	Den som behandlar personuppgifter och bestämmer hur och varför uppgifterna ska behandlas (ändamål och medel för behandlingen).	Artikel 4.7	Avsnitt 2.1
Personuppgiftsbiträde	Den som behandlar personuppgifter på uppdrag av någon annan.	Artikel 4.8	Avsnitt 2.2
Personuppgiftsincident	En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt röjande av eller obehörig åtkomst till personuppgifter.	Artikel 4.12	Avsnitt 15
Register	En strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier.	Artikel 4.6	Avsnitt 1.2.4
Register över behandling	Den personuppgiftsansvariga är skyldig att föra ett register över personuppgiftsbehandlingar.	Artikel 30	Avsnitt 14
Registrerad	Den fysiska person som en personuppgift avser.	Artikel 4.1	Avsnitt 1.2.1
Uppgiftsminimering	Behandling av personuppgifter ska begränsas så långt det är möjligt.	Artikel 5.1 c	Avsnitt 3.3
Tredjeland	Land utanför EU och EES.		Avsnitt 8
Tredje part	En fysisk eller juridisk person som personuppgifter lämnas ut till och som inte är den registrerade, den personuppgiftsansvariga eller personuppgiftsbiträdet.	Artikel 4.10	
Övrig verksamhet på Försäkringskassan	Verksamhet som inte är kärnverksamhet. Det kan till exempel vara personaladministration, lokalförsörjning och SSID (samordnad och säker it-drift).		

Sammanfattning

I den här vägledningen kan du läsa om de bestämmelser i dataskyddsförordningen och socialförsäkringsbalken (SFB) som styr Försäkringskassans behandling av personuppgifter. Även annan viktig lagstiftning och praxis inom området berörs.

Alla medarbetare på Försäkringskassan kommer i sitt arbete på ett eller annat sätt i kontakt med frågor som gäller dataskydd och måste ha kunskap om vad som gäller på detta område. Vägledningen är avsedd att vara ett stöd i vårt löpande arbete. Den ska bidra till att vi hanterar personuppgifter på ett riktigt sätt och att enskilda personer känner att de tryggt kan lämna uppgifter om sig själva till oss.

Läsanvisningar

Vägledningen riktar sig till alla anställda inom Försäkringskassan och till de som på annan grund deltar i vår verksamhet.

Syftet med vägledningen är att öka kunskapen om vad som gäller vid behandling av personuppgifter. Den är tänkt att vara ett stöd i den dagliga hanteringen av uppgifter, men också exempelvis vid utbildning av Försäkringskassans medarbetare och i utvecklingsinsatser.

Vägledningen redovisar och förklarar lagar och andra bestämmelser. Den redogör för de delar av lagens förarbeten som är särskilt viktiga för att förstå hur lagen ska tillämpas. Den redogör också för rättspraxis och för Försäkringskassans rättsliga ställningstaganden.

Hänvisningar

I vägledningen finns hänvisningar till lagar, förordningar och föreskrifter. Det finns också hänvisningar till allmänna råd, Försäkringskassans rättsliga ställningstaganden, interna styrdokument, förarbeten, rättsfall, JK-beslut och andra vägledningar. Dessa hänvisningar finns antingen i löpande text eller inom parentes i direkt anslutning till den mening eller det stycke den avser.

Sist i vägledningen finns en källförteckning som redovisar de lagar, förordningar, domar med mera som nämns i vägledningen.

Att hitta rätt i vägledningen

I vägledningen finns en innehållsförteckning. Den är placerad först och ger en översiktsbild av vägledningens kapitel och avsnitt. Med hjälp av fliken ”Bokmärken” i vänsterkanten kan du navigera mellan avsnitten. Det finns också en sökfunktion för att hitta enstaka ord och begrepp.

1 När ska vi tillämpa bestämmelser om dataskydd?

1.1 Reglering av rätt till skydd för den personliga integriteten

Dataskydd handlar om att skydda den personliga integriteten för den som får sina personuppgifter behandlade. Den enskildes rätt till respekt för sitt privatliv, skydd av sina personuppgifter och skydd mot betydande intrång i den personliga integriteten följer av både Europakonventionen och EU:s rättighetsstadga. Rätten till privatliv uttrycks i artikel 8 i Europakonventionen, som har införts som lag i Sverige (lagen [1994:1219] om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna). I EU:s rättighetsstadga uttrycks rätten till respekt för privat- och familjeliv i artikel 7 och rätten till skydd för personuppgifter i artikel 8. Stadgan är rättsligt bindande för EU:s medlemsstater.

Enligt svensk grundlag är dessutom var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden (2 kap. 6 § RF).

EU har harmoniserat skyddet av personuppgifter genom dataskyddsförordningen, ofta kallad GDPR efter den engelska beteckningen General Data Protection Regulation. En EU-förordning är direkt tillämplig i medlemsländerna, till skillnad från ett EU-direktiv som måste införas genom nationell lagstiftning. Dataskyddsförordningen ska alltså tillämpas i Sverige. Förordningen medför rättigheter och skyldigheter för enskilda och kan åberopas direkt inför en svensk domstol.

Dataskyddsförordningens syfte är att

- skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter
- skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter inom EU så att det fria flödet av uppgifter inom unionen inte hindras (artikel 1 i dataskyddsförordningen).

Utöver dataskyddsförordningen finns flera svenska lagar och förordningar som kompletterar den på olika sätt och stärker skyddet för den personliga integriteten. På Försäkringskassan är det framför allt aktuellt att tillämpa

- dataskyddslagen
- förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning
- 114 kap. SFB
- förordningen (2024:14) om behandling av personuppgifter vid Försäkringskassan och Pensionsmyndigheten
- lagen (2001:99) om den officiella statistiken
- förordningen (2001:100) om den officiella statistiken
- visselblåsarlagen.

Tillämpningsområdet i de olika regleringarna anger när bestämmelser om dataskydd ska tillämpas.

1.2 Dataskyddsförordningens tillämpningsområde

Artikel 2.1 i dataskyddsförordningen
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.

Artikeln anger ramarna för när dataskyddsförordningen ska tillämpas. För att det ska vara möjligt att förstå omfattningen av dataskyddsförordningens tillämpningsområde krävs kännedom om flera olika begrepp och uttryck som används i dataskydds-lagstiftningen. Följande avsnitt redogör för vad en personuppgift är, innebörden av en behandling av personuppgifter, när en behandling ska anses helt eller delvis automatiserad och vad ett register är i dataskyddsförordningens mening.

Tillämpningsområdet inskränks av vissa undantag och en begränsning av det territoriella tillämpningsområdet. Det kan du läsa om i avsnitt 1.2.5 och 1.2.6.

1.2.1 Vad är en personuppgift?

Artikel 4.1 i dataskyddsförordningen
personuppgifter: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad *en registrerad*), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,

Personuppgifter är alla slags uppgifter som på något sätt kan knytas till en fysisk, levande person. Uttrycket ”varje upplysning” i definitionen av begreppet personuppgifter ger begreppet en vid innebörd. Både objektiva och subjektiva upplysningar om en person kan utgöra personuppgifter (EU-domstolens dom Österreichische Datenschutzbehörde och CRIF, C-487/21, EU:C:2023:369, punkt 23). Det kan röra sig om uppgifter om namn, personnummer, adress, telefonnummer och IP-adresser, men även uppgifter om till exempel var personen arbetar, hälsa, ekonomi, partitillhörighet och sexuell läggning. Åsikter och bedömningar som avser en person kan också vara personuppgifter. Vissa typer av personuppgifter kategoriseras som känsliga eller särskilt skyddsvärda (se avsnitt 6). Den person som uppgifterna gäller kallas *registrerad*.

Ofta talas det om direkta och indirekta personuppgifter. En *direkt* personuppgift är en uppgift som ensam kan hänföras till en person, till exempel hens namn eller personnummer. En *indirekt* personuppgift behöver kombineras med andra uppgifter för att det ska vara möjligt att hänföra den till en person. Det kan till exempel vara möjligt att identifiera en person genom en uppgift om vem hen är gift med. Det kan också vara möjligt att identifiera en person utifrån uppgift om till exempel bostadsort och en ovanlig diagnos. Det är inte nödvändigt att just du kan identifiera personen utifrån uppgifterna, utan det är tillräckligt att någon skulle kunna göra det.

Bilder, filmer och ljudfiler är personuppgifter om det är möjligt att identifiera vem som syns eller hörs.

Begreppet personuppgift är alltså väldigt brett. I Försäkringskassans verksamhet är exempelvis namn, personnummer, ärendenummer, ekonomiska uppgifter, hälsouppgifter och användar-id vanligt förekommande personuppgifter.

Uppgifter om juridiska personer är inte personuppgifter. Organisationsnummer är personuppgifter endast om det rör sig om en enskild näringsverksamhet, eftersom organisationsnumret i det fallet utgörs av näringsidkarens personnummer. Uppgifter om fysiska personer som representerar den juridiska personen eller arbetar där är personuppgifter.

Personuppgifter räknas som *anonymiserade* om de har avidentifierats på ett sådant sätt att de inte längre kan hänföras till en fysisk person (skäl 26 i dataskyddsförordningen). För att en personuppgift ska anses anonymiserad krävs att det inte längre är möjligt att avgöra vilken fysisk person som uppgifterna avser, varken genom befintliga uppgifter eller genom att tillföra andra uppgifter. Personuppgifter som har anonymiserats räknas inte längre som personuppgifter, vilket innebär att bestämmelser som gäller behandling av personuppgifter inte är tillämpliga. Viktigt att notera är dock att anonymisering av personuppgifter är en personuppgiftsbehandling som dataskyddsförordningen ska tillämpas på. EDPB har antagit riktlinjer för att klargöra vad anonymisering av personuppgifter innebär (EDPB:s riktlinjer 02/2026 om anonymisering).

Personuppgifter kan även *pseudonymiseras*. Det innebär att det inte längre går att hänföra uppgifterna till en fysisk person utan att kompletterande uppgifter används (artikel 4.5 i dataskyddsförordningen). Pseudonymisering är en säkerhetsåtgärd och innebär inte att uppgifterna upphör att vara personuppgifter. Samtliga regler som gäller behandling av personuppgifter gäller således även pseudonymiserade personuppgifter. Läs mer om pseudonymisering i avsnitt 9.1.1.

Dataskyddsförordningen är som utgångspunkt inte tillämplig på uppgifter om avlidna personer. Enligt 114 kap. 5 § SFB gäller dock socialförsäkringsbalken, dataskydds-förordningen och dataskyddslagen i tillämpliga delar för uppgifter om avlidna personer. Det innebär att om 114 kap. SFB är tillämpligt på en behandling av personuppgifter, ska såväl 114 kap. SFB som dataskyddsförordningen och dataskyddslagen tillämpas i fråga om en avliden persons uppgifter. Bestämmelser som på något sätt kräver den registrerades agerande eller medverkan i övrigt är dock inte tillämpliga på avlidna personer. Efterlevande eller andra kan inte ta över rättigheter som den avlidne hade när hen var i livet (prop. 2019/20:106 s. 32). Det innebär att bestämmelser om rätten till information, rätten till skadestånd och möjligheten att begära rättelse av registrerades personuppgifter inte är tillämpliga i förhållande till en avliden person.

Motsvarande bestämmelser om uppgifter om avlidna personer finns inte i lagen om den officiella statistiken och visselblåsarlagen.

1.2.2 Vad är behandling av personuppgifter?

Artikel 4.2 i dataskyddsförordningen
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,

Behandling av personuppgifter är allt som kan göras med en personuppgift. Det kan

vara både en enskild åtgärd eller en kombination av flera åtgärder. Åtgärden kan vara aktiv eller passiv. Att en personuppgift över huvud taget finns hos Försäkringskassan innebär alltså att personuppgiften behandlas av myndigheten.

Det krävs inte att det är en fysisk person som utför en åtgärd, utan även helt automatiserade åtgärder är behandlingar.

1.2.3 Behandling som sker helt eller delvis automatiskt

Personuppgifter kan behandlas automatiskt eller manuellt. Med automatiskt menas främst behandling som sker digitalt, oavsett vilken digital teknik som används. Manuell behandling är motsatsen till automatisk och avser analog hantering av personuppgifter, exempelvis på papper.

Dataskyddsförordningen gäller vid behandling av personuppgifter som sker helt eller delvis automatiskt. Det innebär att det räcker att en behandling har vissa digitala inslag för att dataskyddsförordningen ska vara tillämplig. Kammarrätten i Stockholm har i en dom bedömt att det rör sig om en delvis automatisk behandling av personuppgifter när kallelser som har överförts från ett digitalt journalsystem skrivs ut och skickas ut via manuell posthantering (KRNS mål nr 5794-23). Även Justitiekanslern anser att karaktären på den bakomliggande behandlingen är avgörande när man bedömer om ett manuellt utlämnande av uppgifter ska anses delvis automatiserat (JK:s beslut dnr 3850-19-4.3.2). Motsatsvis bör det också anses röra sig om en delvis automatisk behandling när en ansökan fylls i på papper i syfte att sedan skannas digitalt. En behandling kan mycket sällan anses vara helt manuell och därmed undantagen från dataskyddsförordningen.

EU-domstolen har uttalat att ett muntligt utlämnande i sig inte är att anse som en automatisk behandling. För att personuppgifter som lämnas ut muntligen ska anses omfattas av bestämmelserna i dataskyddsförordningen krävs enligt domstolen därför att uppgifterna ingår i eller kommer att ingå i ett register (EU-domstolens dom Endemol Shine Finland Oy, C-740/22, EU:C:2024:216, punkt 35). Domen skulle kunna tolkas som att domstolen inte anser att muntligt utlämnande av personuppgifter kan vara en delvis automatisk behandling. Oavsett hur man bör se på detta, omfattas utlämnanden från Försäkringskassan i de allra flesta fall av bestämmelserna i dataskyddsförordningen. Det beror på att våra digitala system även får anses vara register. Läs mer om vad som får anses vara ett register i följande avsnitt.

1.2.4 Behandling i register

Artikel 4.6 i dataskyddsförordningen
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,

I relation till dataskyddsförordningen är ett register en samling av personuppgifter som är strukturerad så att det enkelt går att hitta uppgifter om en person. Även en helt manuell behandling av personuppgifter omfattas av bestämmelserna i dataskyddsförordningen om personuppgifterna ingår i eller kommer att ingå i ett register.

Enligt EU-domstolen krävs det inte att ett register är organiserat på ett visst sätt för att det ska omfattas av regleringen. Definitionen av ett register är därmed ganska vid och innebär att dataskyddsförordningen blir tillämplig för många typer av behandlingar.

Rättsfall

EU-domstolen har i fråga om tolkningen av begreppet *register* enligt det tidigare gällande dataskyddsdirektivet (95/46/EG) uttalat att det inte krävs att det finns särskilda förteckningar eller arrangemang för sökning. Det som är avgörande är om uppgifterna om en person är lätt tillgängliga eller inte. Målet rörde uppgifter i form av minnesanteckningar som hade samlats in av Jehovas vittnen genom dörrknackning. Uppgifterna omfattade information om innehållet i samtal och den besökta personens namn och adress. Syftet med insamlingen av uppgifter var att förbereda senare besök och att administrera förteckningar över personer som inte ville bli besökta. Kriterierna, bland annat besökta personers namn och adress, deras övertygelser eller information om att de inte önskar ta emot besök, hade valts ut på ett sådant sätt att information om en bestämd person kunde tas fram med lätthet. Minnesanteckningarna ansågs därmed omfattas av begreppet register. (EU-domstolens dom Jehovan todistatjat, C-25/17, EU:C:2018:551)

Definitionen av register i det tidigare dataskyddsdirektivet motsvarar definitionen i dataskyddsförordningen och domen från EU-domstolen är därmed fortfarande relevant.

1.2.5 Undantag från det materiella tillämpningsområdet

Dataskyddsförordningen ska enligt artikel 2 inte tillämpas i vissa fall. Inget av de undantag som gäller enligt artikeln är tillämpligt inom ramen för Försäkringskassans verksamhet. Det kan trots detta vara bra att känna till att dataskyddsförordningen inte gäller när privatpersoner behandlar personuppgifter för privata ändamål eller när brottsbekämpande myndigheter behandlar personuppgifter i sin brottsbekämpande verksamhet.

För brottsbekämpande verksamhet finns ett särskilt EU-direktiv som gäller behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder. Direktivet har implementerats i Sverige genom brottsdatalagen (2018:1177). Brottsdatalagen är inte tillämplig inom ramen för Försäkringskassans verksamhet (jfr 1 kap. 6 § brottsdatalagen).

1.2.6 Territoriellt tillämpningsområde

Artikel 3.1 i dataskyddsförordningen

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.

Dataskyddsförordningen gäller om en personuppgiftsansvarig eller ett personuppgiftsbiträde har ett verksamhetsställe inom EU/EES och behandlar personuppgifter i samband med den verksamheten. Som framgår av artikeln krävs inte att behandlingen i sig utförs inom EU/EES för att dataskyddsförordningen ska bli tillämplig.

Om den personuppgiftsansvariga eller ett personuppgiftsbiträde inte har ett verksamhetsställe inom EU/EES, kan dataskyddsförordningen ändå vara tillämplig om de erbjuder varor och tjänster till registrerade som befinner sig inom EU/EES.

Länder utanför EU/EES kallas normalt för tredjeland. Läs mer om tredjeland och överföring av personuppgifter till tredjeland i avsnitt 8.

1.3 Reglering som kompletterar dataskyddsförordningen

Dataskyddsförordningens bestämmelser gäller alltid om en behandling av personuppgifter omfattas av förordningens tillämpningsområde. Det gäller även om en annan dataskyddsreglering samtidigt är tillämplig för behandlingen.

Dataskyddsförordningen kompletteras på olika sätt av svenska bestämmelser, som till exempel specificerar eller begränsar vad som är en tillåten behandling. Genom sådana kompletterande bestämmelser stärks skyddet för den personliga integriteten.

I dataskyddslagen finns generella kompletterande bestämmelser. Den gäller när det inte finns mer specifika bestämmelser för ett visst område. Om en annan lag eller en förordning innehåller någon bestämmelse som avviker från dataskyddslagen, ska den avvikande bestämmelsen tillämpas i stället (1 kap. 6 § dataskyddslagen).

Det finns också dataskyddsregleringar som gäller för ett begränsat tillämpningsområde. Sådana regleringar kallas ofta *registerförfattningar*. För Försäkringskassans verksamhet gäller framför allt 114 kap. SFB och förordningen (2024:14) om behandling av personuppgifter vid Försäkringskassan och Pensionsmyndigheten, men det kan även vara aktuellt att tillämpa lagen om den officiella statistiken och 7 kap. visselblåsarlagen.

Förvaltningslagen kompletterar dataskyddsförordningen vid hantering av ärenden som inleds till följd av att registrerade utövar sina rättigheter.

Läs mer
Läs mer om bestämmelser i förvaltningslagen i Försäkringskassans vägledning (2004:7) *Förvaltningsrätt i praktiken*.

1.3.1 Tillämpningsområdet för 114 kap. SFB

114 kap. 2 § SFB
Detta kapitel gäller vid behandling av personuppgifter i verksamhet som avser förmåner enligt denna balk samt andra förmåner och ersättningar som enligt lag eller förordning eller särskilt beslut av regeringen handläggs av Försäkringskassan eller Pensionsmyndigheten.

Kapitlet gäller endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller kommer att ingå i ett register.

Bestämmelserna i 114 kap. SFB ska tillämpas vid behandling av personuppgifter inom Försäkringskassans kärnverksamhet.

Sådana förmåner och ersättningar som inte regleras i SFB men som handläggs av Försäkringskassan är bland annat aktivitetsstöd och ersättning till totalförsvarspliktiga. Även behandling av personuppgifter i Försäkringskassans register över godkända utförare för fritidskortet faller inom tillämpningsområdet för 114 kap. SFB (prop. 2024/25:157 s. 101).

I likhet med dataskyddsförordningen gäller 114 kap. SFB vid behandling av personuppgifter som är helt eller devis automatiserad och vid manuell behandling av personuppgifter om de ingår, eller kommer att ingå, i ett register. Innebörden av begreppen helt eller delvis automatiserad behandling, manuell behandling och register är desamma som enligt dataskyddsförordningen (avsnitt 1.2.3 och 1.2.4).

Rent administrativ verksamhet utan någon koppling till förmånssystemet omfattas inte av tillämpningsområdet för 114 kap. (prop. 2002/03:135 s. 43 f.). Det kan exempelvis handla om personuppgifter som behandlas i den personaladministrativa verksamheten. Inte heller verksamhet som tillämpar lagen om den officiella statistiken omfattas av tillämpningsområdet för 114 kap. SFB (prop. 2023/24:29 s. 22).

Vid uppföljning av rehabinsatser som finansieras av samordningsförbund (Finsam) omfattas enbart sådana personuppgifter som avser personer som har ett förmånsärende hos Försäkringskassan av tillämpningsområdet för 114 kap. SFB.

1.3.2 Tillämpningsområdet för lagen om den officiella statistiken

1 § lagen om den officiella statistiken
Denna lag innehåller bestämmelser om officiell statistik.

Regeringen meddelar föreskrifter om vilka myndigheter som ansvarar för officiell statistik (statistikansvariga myndigheter).

Bestämmelserna i 14–16 och 19 §§ gäller även vid framställning av annan statistik hos en statistikansvarig myndighet.

Försäkringskassan är statistikansvarig myndighet och ansvarar för att utveckla, producera och tillgängliggöra officiell statistik inom områdena *Stöd till familjer och barn* och *Stöd vid sjukdom och funktionsnedsättning* (bilagan till förordningen om den officiella statistiken). Därutöver framställer vi statistik som en del i myndighetens uppdrag att följa, analysera och förmedla socialförsäkringssystemets utveckling och effekter för enskilda och samhälle (2 § 6 förordningen [2009:1174] med instruktion för Försäkringskassan). Statistik kan också framställas för internt bruk, till exempel för att planera och följa upp verksamheten eller för att handlägga ärenden. Det förekommer dessutom att Försäkringskassan får i uppdrag att ta fram statistik åt en annan aktör, till exempel en myndighet eller en forskare.

Vid framställning av officiell statistik och annan statistik inom den särskilda statistikverksamheten på Försäkringskassan gäller lagen och förordningen om den officiella statistiken. I dessa författningar finns särskilda bestämmelser om behandling av personuppgifter som gäller utöver dataskyddsförordningen och dataskyddslagen. När statistik framställs i kärnverksamheten tillämpas 114 kap. SFB (se avsnitt 5.1.6).

Läs mer
Läs mer om Försäkringskassans särskilda statistikverksamhet i vägledningen (2001:3) *Offentlighet, sekretess och utlämnande av handlingar och uppgifter*.

1.3.3 Tillämpningsområdet för 7 kap. visselblåsarlagen

7 kap. 1 § visselblåsarlagen
Bestämmelserna i detta kapitel gäller vid behandling av personuppgifter i ett uppföljningsärende.

Bestämmelserna tillämpas endast på helt eller delvis automatiserad behandling av personuppgifter och annan behandling av personuppgifter som ingår eller kommer att ingå i ett register.

Sverige har genom visselblåsarlagen genomfört Europaparlamentets och rådets direktiv (EU) 2019/1937 av den 23 oktober 2019 om skydd för personer som rapporterar om överträdelser av unionsrätten (visselblåsardirektivet). Visselblåsarlagen gäller vid rapportering i ett arbetsrelaterat sammanhang av information om missförhållanden som det finns ett allmänintresse av att de kommer fram (1 kap. 2 § visselblåsarlagen).

Rapporterade missförhållanden hanteras inom ramen för så kallade uppföljningsärenden.

7 kap. visselblåsarlagen gäller vid behandling av personuppgifter i ett uppföljningsärende. I likhet med dataskyddsförordningen gäller kapitlet vid behandling av personuppgifter som är helt eller devis automatiserad och vid manuell behandling av personuppgifter om de ingår, eller kommer att ingå, i ett register. Innebörden av begreppen helt eller delvis automatiserad behandling, manuell behandling och register är desamma som enligt dataskyddsförordningen (avsnitt 1.2.3 och 1.2.4).

Läs mer

Läs mer om uppföljningsärenden i Försäkringskassans anvisningar (2023:07) *Försäkringskassans visselblåsarfunktion*.

2 Roller och ansvar

I dataskyddsförordningen föreskrivs ett antal rättigheter för den som får sina personuppgifter behandlade (den registrerade) och skyldigheter för den som ansvarar för behandlingen. Den personuppgiftsansvariga är ytterst ansvarig för en behandling.

I vissa fall behandlar någon annan personuppgifter för den personuppgiftsansvarigas räkning. Den som gör det kallas personuppgiftsbiträde.

Syftet med begreppen personuppgiftsansvarig och personuppgiftsbiträde är att fördela ansvaret för behandlingen. Det är viktigt att aldrig påbörja en behandling innan ansvarsfördelningen har fastställts för att inga skyldigheter ska falla mellan stolarna och för att den enskilde ska kunna få sina rättigheter tillgodosedda.

Vissa personuppgiftsansvariga och personuppgiftsbiträden, bland annat myndigheter, måste utse dataskyddsombud. Dataskyddsombudet ansvarar inte för behandlingen av personuppgifter, utan ska bland annat övervaka att organisationen följer dataskydds-förordningen.

2.1 Personuppgiftsansvarig

Artikel 4.7 i dataskyddsförordningen
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 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,

Enligt huvudregeln i dataskyddsförordningen är den som bestämmer ändamålen och medlen för behandlingen av personuppgifter personuppgiftsansvarig. Den personuppgiftsansvariga kan dock också utses i nationell rätt. Det är vanligt i så kallade registerförfattningar.

Bedömningen av vem som bestämmer ändamålen och medlen ska göras utifrån de faktiska omständigheterna i det enskilda fallet. Vid bedömningen av vem som får anses bestämma ändamålen är anledningen till behandlingen och vem som har tagit initiativet till den avgörande. Den som avgör hur behandlingen ska gå till, till exempel vilken teknik som ska användas, får anses bestämma medlen för behandlingen.

Vissa mer praktiska aspekter kan överlåtas till ett personuppgiftsbiträde att besluta om. Det kan handla om till exempel valet av en viss typ av maskin eller programvara eller detaljerade säkerhetsåtgärder (så kallade ”icke-väsentliga medel”) (EDPB:s riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, s. 16).

Enligt Högsta förvaltningsdomstolen (HFD) förutsätter ett personuppgiftsansvar att den som bestämmer ändamål och medel för behandlingen också utför behandlingen, det vill säga vidtar åtgärder som innefattar behandling, eller att sådana åtgärder utförs för dennes räkning (HFD 2012 ref. 21).

Den som i praktiken bestämmer ändamål och medel för behandlingen kommer att anses vara personuppgiftsansvarig även om den i ett avtal med någon annan pekas ut som

personuppgiftsbiträde (jämför EDPB:s riktlinjer angående begreppen personuppgifts-ansvarig och personuppgiftsbiträde, s. 14). Den som uttryckligen har motsatt sig en viss behandling är dock inte ansvarig för behandlingen, om den trots detta ändå kommer till stånd (EU-domstolens dom Nacionalinis visuomenės sveikatos centras, C-683/21, EU:C:2023:949, punkt 38).

Om en behandling av personuppgifter syftar till att uppfylla ett författningsreglerat krav, är den som enligt författningen ska uppfylla kravet normalt personuppgiftsansvarig för behandlingen (EDPB:s riktlinjer angående begreppen personuppgiftsansvarig och personuppgiftsbiträde, s. 13).

Ett personuppgiftsansvar förutsätter inte åtkomst till de personuppgifter som behandlas. När en myndighet tillhandahåller elektroniska självbetjäningstjänster kan myndigheten exempelvis vara personuppgiftsansvarig för uppgifter som lämnas via tjänsten, även innan de blivit tillgängliga för myndigheten.

Rättsfall

I fråga om elektroniska självbetjäningstjänster i form av anmälan av tillfällig föräldrapenning via sms och arbetsgivares anmälan av sjukfall via en så kallad infratjänst ansåg HFD att Försäkringskassan var personuppgiftsansvarig för den behandling som skedde innan uppgifterna blev tillgängliga för myndigheten. Försäkringskassan ansågs ha bestämt såväl ändamål som medel för behandlingen trots att vi saknade möjlighet att påverka hur uppgifterna hanterades innan de blev tillgängliga för oss. (HFD 2012 ref. 21)

Försäkringskassans personuppgiftsansvar

114 kap. 7 § SFB

Försäkringskassan och Pensionsmyndigheten är personuppgiftsansvariga för behandling av personuppgifter i sina respektive verksamheter.

I vissa fall kan den personuppgiftsansvariga utses i nationell rätt. Försäkringskassan och Pensionsmyndigheten är exempelvis personuppgiftsansvariga för behandling av personuppgifter i sina respektive verksamheter. Det reglerade personuppgiftsansvaret för Försäkringskassan omfattar den verksamhet som ryms inom tillämpningsområdet för 114 kap. SFB (se avsnitt 1.3.1).

När Försäkringskassan behandlar personuppgifter för Pensionsmyndighetens räkning kan behandlingen i vissa fall omfattas av tillämpningsområdet för 114 kap. SFB, eftersom behandlingen sker inom ramen för en förmån enligt SFB. För att Försäkringskassan ska anses vara personuppgiftsansvarig krävs dock att behandlingen utförs för ändamål i vår egen verksamhet. När det finns ett författningsreglerat ansvar för Försäkringskassan att ta över viss handläggning från Pensionsmyndigheten, är Försäkringskassan personuppgiftsansvarig för behandlingen (jämför 108 kap. 14 a § SFB).

På Försäkringskassan är avdelningscheferna informationsägare, vilket innefattar ett ansvar för behandlingen av personuppgifter inom avdelningen (avsnitt 4.2.2 i Generaldirektörens arbetsordning). Detta är dock en intern arbets- och ansvarsfördelning. Försäkringskassan är alltid personuppgiftsansvarig i den mening som avses i dataskyddsregleringen. Det innebär att det vid tillämpningen av dataskyddsbestämmelser är Försäkringskassan och inte en enskild avdelning som är personuppgiftsansvarig.

Gemensamt personuppgiftsansvar

Artikel 26.1 i dataskyddsförordningen
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.

Ibland kan det finnas fler än en personuppgiftsansvarig för en behandling. Om flera aktörer bestämmer ändamål och medel för en viss behandling, kan de vara gemensamt personuppgiftsansvariga.

Ett viktigt kriterium för att det ska anses handla om ett gemensamt personuppgifts-ansvar är att behandlingen inte skulle vara möjlig utan båda parternas deltagande i ändamålen och medlen (EDPB:s riktlinjer angående begreppen personuppgiftsansvarig och personuppgiftsbiträde, s. 21). Att en av parterna inte har tillgång till personuppgifter som behandlas är inte tillräckligt för att utesluta gemensamt ansvar (EU-domstolens dom Wirtschaftsakademie, C-210/16, EU:C:2018:388, punkt 38).

Omständigheten att det finns ett gemensamt personuppgiftsansvar behöver inte innebära att alla har ett likvärdigt ansvar (EDPB:s riktlinjer angående begreppen personuppgiftsansvarig och personuppgiftsbiträde, s. 21). Om de inblandade är involverade i olika skeden av behandlingen av personuppgifter och i olika utsträckning, ska ansvaret för var och en av dem bedömas med beaktande av alla relevanta omständigheter i fråga (EU-domstolens dom IAB Europe, C-604/22, EU:C:2024:214, punkt 58).

Att samma uppgifter om en person förekommer hos olika myndigheter måste inte betyda att det finns ett gemensamt personuppgiftsansvar. Var och en av myndigheterna kan ensamt vara personuppgiftsansvarig för sin behandling.

När Försäkringskassan är gemensamt personuppgiftsansvarig tillsammans med en annan aktör, kan det vara lämpligt att ingå ett datadelningsavtal. Avtalet kan bl.a. ange ansvarsfördelningen och tillåten personuppgiftsbehandling. Det kan också tillämpas som rättslig grund enligt artikel 6 i dataskyddsförordningen vid sådan personuppgiftsbehandling som är en följd av det gemensamma personuppgiftsansvaret.

2.2 Personuppgiftsbiträde

Artikel 4.8 i dataskyddsförordningen
personuppgiftsbiträde: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,

Den som behandlar personuppgifter för någon annans räkning kan vara ett personuppgiftsbiträde. För att en aktör ska räknas som ett personuppgiftsbiträde krävs

att aktören intar en osjälvständig roll och saknar rätt att bestämma ändamålen med och medlen för behandlingen. Personuppgiftsbiträdet får inte behandla uppgifterna på annat sätt än enligt den personuppgiftsansvarigas instruktioner.

Ett personuppgiftsbiträde finns alltid utanför Försäkringskassans organisation. Konsulter som utför arbete under vårt direkta ansvar, på samma sätt som anställda, ses som en del av vår organisation och vårt ansvar som personuppgiftsansvarig.

Exempel på personuppgiftsbiträden kan vara en enskild leverantör av tjänster eller en myndighet som utför arbete åt en annan aktör. Exempelvis behandlar Statens servicecenter personuppgifter för Försäkringskassans räkning och Försäkringskassan behandlar personuppgifter för Pensionsmyndighetens räkning. Den som får personuppgifter från Försäkringskassan i syfte att använda uppgifterna för ändamål i sin egen verksamhet är inte ett personuppgiftsbiträde i detta avseende.

När Försäkringskassan anlitar ett personuppgiftsbiträde ska behandlingen regleras i ett särskilt personuppgiftsbiträdesavtal (se avsnitt 10).

2.3 Dataskyddsombud

Artikel 37.1 a i dataskyddsförordningen
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,

Det följer av dataskyddsförordningen att Försäkringskassan måste utnämna ett dataskyddsombud. Hens övergripande och viktigaste uppgift är att övervaka att vi följer dataskyddsförordningen. Ansvaret för att vi faktiskt gör det ligger dock alltid hos Försäkringskassan i egenskap av personuppgiftsansvarig eller personuppgiftsbiträde.

Den personuppgiftsansvariga och personuppgiftsbiträdet ska aktivt och i god tid involvera dataskyddsombudet i alla frågor gällande dataskydd och säkerställa att hen har tillräckliga resurser för att utföra sina uppgifter (artikel 38.1 och 2 i dataskyddsförordningen).

Dataskyddsombudet ska övervaka om dataskyddsbestämmelserna följs och informera och ge råd enligt dataskyddsregelverket, bland annat vid konsekvensbedömningar. Hen ska också samarbeta med IMY, som är tillsynsmyndighet, och fungera som kontakt-person för IMY vid bland annat förhandssamråd (artikel 39.1 i dataskyddsförordningen).

Dataskyddsombudet ska ha en oberoende roll och ges förutsättningar att utföra sina arbetsuppgifter självständigt. Enligt artikel 38.3 i dataskyddsförordningen får hen inte avsättas eller bli föremål för sanktioner för att ha utfört sina arbetsuppgifter. Den personuppgiftsansvariga ska särskilt säkerställa att dataskyddsombudet inte instrueras i hur uppdraget fullgörs, till exempel vilka resultat som bör uppnås, hur ett klagomål ska utredas eller om IMY ska rådfrågas. Dataskyddsombudet får inte heller instrueras att inta en viss ståndpunkt i frågor som rör dataskyddslagstiftningen, till exempel en viss tolkning av lagen (Artikel 29-gruppens riktlinjer om dataskyddsombud [WP 243 rev.01], s. 17).

Dataskyddsombudet ska rapportera direkt till högsta förvaltningsnivå, vilket hos Försäkringskassan är styrelsen och generaldirektören (artikel 38.3 i dataskyddsförordningen).

I avsnitt 12.4 i Generaldirektörens arbetsordning står det att dataskyddsombudet hos Försäkringskassan har rätt till tillgång till de uppgifter som rör Försäkringskassan och som behövs för att dataskyddsombudet ska kunna fullgöra sina uppgifter.

3 Grundläggande principer för behandling av personuppgifter

För all behandling av personuppgifter gäller enligt artikel 5 i dataskyddsförordningen de grundläggande principerna om

- laglighet, korrekthet och öppenhet
- ändamålsbegränsning
- uppgiftsminimering
- riktighet
- lagringsminimering
- integritet och konfidentialitet
- ansvarsskyldighet.

De grundläggande principerna är kärnan i dataskyddsförordningen. De sätter de yttersta ramarna för vad som är en tillåten behandling och säkerställer att personuppgifter hanteras ansvarsfullt, säkert och med respekt för individens integritet. Samtliga principer ska vara uppfylla vid behandling av personuppgifter.

3.1 Laglighet, korrekthet och öppenhet

Artikel 5.1 a i dataskyddsförordningen
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*).

Laglighet

EU-domstolen har uttalat att framför allt artiklarna 5–11 i dataskyddsförordningen måste följas för att behandlingen ska anses laglig (EU-domstolens dom UZ, C-60/22, EU:C:2023:373, punkt 57–66). Främst innebär principen om laglighet att all personuppgiftsbehandling måste ske med stöd av en rättslig grund enligt artikel 6 i dataskyddsförordningen (prop. 2017/18:105 s. 47). Vilka de rättsliga grunderna är framgår av avsnitt 4.

HFD har vid tillämpning av den tidigare personuppgiftslagen ansett att kravet på laglighet ska tolkas på så sätt att behandlingen ska vara förenlig med bestämmelserna i den lagen och med föreskrifter som har meddelats med stöd av den. Omständigheten att en planerad behandling kan komma att strida mot en annan lag ansågs inte innebära att den också kommer i konflikt med kravet på laglighet i personuppgiftslagen (HFD 2016 ref. 40). Justitiekanslern har kommit till motsvarande slutsats i fråga om dataskyddsförordningen (JK dnr 2023/9812).

Korrekthet

Principen om korrekthet innebär att behandlingen av personuppgifter ska vara rättvis, skälig, rimlig och proportionerlig i förhållande till de registrerade. Behandlingen ska också vara begriplig för de registrerade och inte ske på dolda eller manipulerande sätt (IMY.se om grundläggande principer).

En personuppgiftsbehandling ska ske på ett sätt som den registrerade rimligen kan förvänta sig och den personuppgiftsansvariga bör beakta bland annat eventuell

maktobalans mellan sig och den registrerade. Den registrerade måste också kunna kommunicera med den personuppgiftsansvariga och utöva sina rättigheter i samband med behandling av hens personuppgifter (EDPB:s riktlinjer 4/2019 om artikel 25 Inbyggt dataskydd och dataskydd som standard, s. 18–19).

För att det ska vara möjligt att avgöra om kravet på korrekthet är uppfyllt, bör det göras en intresseavvägning. Det innebär att Försäkringskassan ska göra en avvägning mellan behovet av att behandla personuppgifter och de eventuella integritets- och säkerhetsrisker som kan uppkomma till följd av behandlingen. För att det ska vara försvarligt eller proportionerligt ska fördelarna med behandlingen överväga riskerna. Särskild hänsyn ska tas till om behandlingen omfattar känsliga personuppgifter och sårbara personer. Det kan vara oförenligt med principen om korrekthet att vidta en viss behandlingsåtgärd om behandlingen är oskälig i förhållande till den registrerade, även om kravet på en rättslig grund är uppfyllt (prop. 2017/18:105 s. 47).

Öppenhet

Principen om öppenhet innebär att det ska vara klart och tydligt för registrerade hur personuppgifter som rör dem samlas in och behandlas i övrigt. All information och kommunikation i samband med personuppgiftsbehandlingen ska vara lättillgänglig och lättbegriplig och ett klart och tydligt språk ska användas (skäl 39 till dataskydds-förordningen).

I artiklarna 13–15 i dataskyddsförordningen om rätten till information och tillgång preciseras innebörden av öppenhetsprincipen (avsnitt 11).

Kravet att informationen ska vara begriplig innebär att den bör kunna förstås av en genomsnittsmedlem av den avsedda målgruppen. Om den personuppgiftsansvariga är medveten om att målgruppen omfattar utsatta personer i samhället, bland annat barn och personer med funktionsnedsättning, bör sårbarhet hos sådana registrerade beaktas vid bedömningen av hur principen om öppenhet ska säkerställas. (Artikel 29-gruppens riktlinjer om öppenhet enligt förordning 2016/679 [WP260 rev.01])

3.2 Ändamålsbegränsning

Artikel 5.1 b i dataskyddsförordningen
Vid behandling av personuppgifter ska följande gälla:

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).

Principen om ändamålsbegränsning är grundläggande vid all personuppgiftsbehandling. Personuppgifter får bara samlas in om ett eller flera ändamål för behandlingen har fastställts vid insamlingstidpunkten.

Uttrycket ”samlas in” definieras inte i dataskyddsförordningen. Det får antas att det avser samtliga sätt genom vilka Försäkringskassan får tillgång till personuppgifter (jfr Öman, *Dataskyddsförordningen [GDPR] m.m. En kommentar*, JUNO Version 4, kommentaren till artikel 5).

Det är som utgångspunkt den personuppgiftsansvariga som bestämmer för vilka ändamål som personuppgifterna ska behandlas. Detta framgår redan av definitionen av

personuppgiftsansvarig (avsnitt 2.1). Ändamål kan dock även fastställas i författning. Det har exempelvis fastställts tillåtna ändamål inom Försäkringskassans kärnverksamhet i 114 kap. SFB.

Att ändamålen ska vara *särskilda* innebär att de ska ha en viss grad av precision. Det ska vara möjligt att utifrån det aktuella ändamålet avgöra vilken behandling som kommer att förekomma. Om ändamålet inte är tillräckligt preciserat är det inte möjligt att bedöma om personuppgifterna är adekvata, relevanta och inte för omfattande i förhållande till ändamålet (jämför principen om uppgiftsminimering).

Det är möjligt att ange flera olika ändamål vid den tidpunkt då personuppgifterna samlas in (jämför artikel 89.4 i dataskyddsförordningen). De olika ändamålen måste inte vara förenliga med varandra. Uppgifter kan alltså samlas in för flera helt olika ändamål, som saknar koppling till varandra.

Kravet på att ändamål ska vara uttryckligt angivna uppfylls bland annat genom dokumentation av personuppgiftsbehandlingar (avsnitt 14) och information till registrerade (avsnitt 11).

Principen om att ändamål ska vara berättigade har i likhet med principen om laglighet en direkt koppling till de rättsliga grunderna i artikel 6.1. Ett ändamål som inte är berättigat i förhållande till en rättslig grund är inte förenligt med artikel 5 i dataskyddsförordningen (prop. 2017/18:105 s. 47).

Se vidare avsnitt 5 om ändamål.

Finalitetsprincipen

Finalitetsprincipen innebär att personuppgifter som har samlats in för ett visst ändamål inte får behandlas för ett annat ändamål som är oförenligt med det ursprungliga ändamålet.

I likhet med övriga grundläggande principer gäller finalitetsprincipen vid all behandling av personuppgifter. Av tydlighetsskäl har lagstiftaren dock valt att införa bestämmelser som ger uttryck för finalitetsprincipen i många registerförfattningar, bland annat 114 kap. SFB. Läs mer om hur finalitetsprincipen förhåller sig till bestämmelserna i 114 kap. SFB i avsnitt 5.1.9.

Vi ska bedöma om behandlingen av personuppgifter är förenlig med finalitetsprincipen genom att bland annat beakta:

- kopplingar mellan de ändamål för vilka personuppgifterna har samlats in och ändamålen med den planerade vidarebehandlingen
- det sammanhang inom vilket personuppgifterna har samlats in
- personuppgifternas art
- eventuella konsekvenser för registrerade av den planerade vidarebehandlingen
- förekomsten av lämpliga skyddsåtgärder.

De registrerades rimliga förväntningar bör också vara en faktor när vi prövar om ändamålet är oförenligt med det ursprungliga ändamålet (jämför Artikel 29-gruppens yttrande 3/2013 om ändamålsbestämning enligt dataskyddsdirektivet, WP 203, s. 24 f.).

I vissa fall krävs ingen bedömning utifrån finalitetsprincipen. Vidarebehandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål enligt artikel 89.1 i dataskyddsförordningen anses alltid vara förenlig med finalitetsprincipen. Det är även tillåtet att behandla personuppgifter med stöd av EU-rätt eller nationell lagstiftning, även om de nya ändamålen är oförenliga med de

ursprungliga ändamålen (artikel 6.4 i dataskyddsförordningen). Ett exempel på sådan nationell lagstiftning är uppgiftsskyldigheter. När det i lag eller förordning föreskrivs att uppgifter ska lämnas får lagstiftaren anses ha tagit ställning till att uppgiftslämnandet är nödvändigt och proportionerligt (prop. 2023/24:29 s. 47 f.).

Rättsfall
Enligt HFD behöver myndigheter inte, utöver sekretessprövningen, ta ställning till om ett utlämnande av personuppgifter enligt 6 kap. 5 § OSL är förenligt med de ändamål som personuppgifterna har samlats in för (HFD 2021 ref. 10).

För utlämnande med stöd av offentlighetsprincipen, se avsnitt 7.3.

3.3 Uppgiftsminimering

Artikel 5.1 c i dataskyddsförordningen
Vid behandling av personuppgifter ska följande gälla:

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

Principen om uppgiftsminimering avser att skydda enskildas personliga integritet genom att begränsa behandlingen av personuppgifter. Vi bör behandla personuppgifter endast om syftet med behandlingen inte rimligen kan uppnås genom andra medel (skäl 39 till dataskyddsförordningen). Det är inte tillåtet att samla in personuppgifter "för säkerhets skull" eller för potentiell framtida användning utan uppgifterna ska vara av direkt betydelse för det angivna ändamålet.

Personuppgifterna får inte heller vara för omfattande i förhållande till det angivna ändamålet. Om vi kan uppnå syftet med en behandling på ett sätt som kräver färre personuppgifter eller inga personuppgifter alls, ska vi välja det före ett tillvägagångssätt som kräver mer omfattande behandling av personuppgifter. Ibland kan det till exempel räcka med statistik för en hel grupp i stället för information på individnivå. Det är också viktigt att förhindra onödig spridning av personuppgifter.

Principen om uppgiftsminimering innebär enligt EU-domstolen även att den personuppgiftsansvariga är skyldig att begränsa perioden för insamling av personuppgifter till vad som är absolut nödvändigt (se bland annat EU-domstolens dom Schrems, C-446/21, EU:C:2024:834, punkt 52). Det innebär att man inte får samla in personuppgifter kontinuerligt, om det inte är absolut nödvändigt med hänsyn till ändamålet.

3.4 Riktighet

Artikel 5.1 d i dataskyddsförordningen
Vid behandling av personuppgifter ska följande gälla:

d) De ska vara riktiga 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 (riktighet).

Av principen om riktighet följer att personuppgifter ska vara riktiga och ge en rättvisande

bild av de förhållanden som uppgiften avser. Uppgifterna ska också vara uppdaterade, om det är nödvändigt.

Vi ska bedöma personuppgifters riktighet i förhållande till det ändamål för vilket de samlades in. Om det vid tillfället för registreringen av en uppgift har funnits en avsikt eller en tanke bakom registreringen bör vi utgå från att den är riktig.

Om ändamålet för behandlingen är att registrera inkomna uppgifter, ska de personuppgifter som vi registrerar anses riktiga om de stämmer överens med de inkomna uppgifterna. Det gäller oavsett om de registrerade uppgifterna överensstämmer med verkligheten eller inte (jämför JK:s beslut dnr 2022/1169). En personuppgift som inte återger en korrekt bild av en omständighet bör som utgångspunkt inte anses vara oriktig och kräva rättning om den korrekt återger ett händelseförlopp i verksamheten och dessutom behövs i verksamheten (jämför SOU 1999:105 s. 286). Uppgifter i en inkommen allmän handling ska därför normalt sett inte anses felaktiga i dataskyddsrättsligt perspektiv, även om de inte överensstämmer med verkligheten. Om uppgifterna med hänsyn till ändamålet med behandlingen är ofullständiga, kan de ofta rättas genom komplettering.

Registreringar som är ett resultat av att en tjänsteman har gjort en felaktig rättslig bedömning eller liknande har av Justitiekanslern normalt inte ansetts som felaktiga i personuppgiftslagens mening (JK:s beslut dnr 2937-04-42).

Vi måste vidta alla rimliga åtgärder för att säkerställa att personuppgifter som är felaktiga raderas eller rättas utan dröjsmål. Vilka åtgärder som är rimliga får bedömas mot bakgrund av omständigheterna i varje enskilt fall, såsom ändamålen för behandlingen av personuppgifter, hur många personuppgifter som behandlas och vilka konsekvenser en felaktig personuppgift kan få för den registrerade. Vi ska bedöma vad som är ett dröjsmål i relation till den tidpunkt då vi fick kännedom om att personuppgifterna var felaktiga. (Öman, *Dataskyddsförordningen [GDPR] m.m. En kommentar*, JUNO Version 4, kommentaren till artikel 5)

Se avsnitt 12.1 och 12.2 om rättelse och radering.

Rättsfall

En uppgift om den registrerades könsidentitet vid födseln är felaktig om den registrerade i dag anser sig ha en annan könsidentitet och ändamålet för behandlingen är att identifiera den registrerade (EU-domstolens dom Deldits, C-247/23, EU:C:2025:172, punkt 26 och 32).

Kammarrätten i Jönköping har ansett att journalanteckningar som på ett riktigt sätt återger vilka bedömningar som läkare och andra gjorde vid tiden för införandet i en patientjournal inte ska anses vara en sådan oriktig uppgift som ska rättas enligt artikel 16 i dataskyddsförordningen. Som skäl för detta har angetts att det är fråga om bedömningar, oavsett om bedömningarna är felaktiga eller inte. (KRNJ 2745-19)

3.5 Lagringsminimering

Artikel 5.1 e i dataskyddsförordningen
Vid behandling av personuppgifter ska följande gälla:

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).

Utgångspunkten enligt dataskyddsförordningen är att personuppgifter inte ska behandlas längre tid än vad som är nödvändigt för det fastställda ändamålet för personuppgiftsbehandlingen. Därefter ska personuppgifterna raderas eller anonymiseras, så att de inte längre är personuppgifter.

Personuppgifter får dock lagras under längre perioder i den mån de enbart behandlas för bland annat arkivändamål av allmänt intresse. Sådan behandling behöver inte vara förenlig med det ursprungliga ändamålet (jämför avsnittet om finalitetsprincipen i avsnitt 3.2).

Försäkringskassans behandling av personuppgifter för arkivändamål sker med stöd av arkivlagen. Utgångspunkten i arkivlagen är att allmänna handlingar ska bevaras men under vissa förutsättningar får gallras (10 § arkivlagen [1990:782]). Bestämmelser om gallring har ett annat syfte än dataskyddsförordningens krav på lagringsminimering. Syftet med gallringsbestämmelser är att begränsa arkivens omfattning medan bestämmelser om hur länge personuppgifter får behandlas syftar till att skydda enskildas personliga integritet.

Arkivlagens regler gäller bara så länge det inte har införts särskilda bestämmelser om gallring i annan lag eller förordning eller föreskrifter som beslutats av Riksarkivet (10 § tredje stycket arkivlagen). Bestämmelser om hur länge personuppgifter får behandlas är inte sådana särskilda bestämmelser om gallring och gäller därmed inte före arkivlagens bestämmelser.

Enligt 14 § arkivförordningen (1991:446) får statliga myndigheter gallra allmänna handlingar endast i enlighet med föreskrifter eller beslut av Riksarkivet om inte särskilda gallringsföreskrifter finns i lag eller förordning. I Försäkringskassans kärnverksamhet finns en särskild gallringsbestämmelse i 114 kap. 15 § SFB. Undantag från kravet på gallring inom kärnverksamheten beslutas av Riksarkivet med stöd av 7 § förordningen om behandling av personuppgifter vid Försäkringskassan och Pensionsmyndigheten.

Läs mer
Läs mer om gallring i Försäkringskassans vägledning (2026:3) *Hantering av verksamhetsinformation och arkiv*, Försäkringskassans riktlinjer (2022:01) *Gallring och bevarande av verksamhetsinformation* och Försäkringskassans anvisningar (2023:09) *Gallring och bevarande av verksamhetsinformation*.

3.6 Integritet och konfidentialitet

Artikel 5.1 f i dataskyddsförordningen
Vid behandling av personuppgifter ska följande gälla:

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).

När vi behandlar personuppgifter ska vi skydda dem genom att använda lämpliga tekniska eller organisatoriska åtgärder. Kravet på lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen av personuppgifter utförs i enlighet med dataskyddsförordningen framgår även av artikel 24, 25 och 32 i dataskyddsförordningen. Läs mer i avsnitt 9.

Rättsfall
Kammarrätten i Stockholm fastställde en sanktionsavgift om fyra miljoner kronor för utbildningsnämnden i Stockholms stad för att personuppgifter i den så kallade Skolplattformen behandlats i strid med bland annat artikel 5.1 f och artikel 32.1 i dataskyddsförordningen. Överträdelserna bestod i att det på grund av tekniska brister, och beträffande ett delsystem även organisatoriska brister, fanns möjlighet att ta del av information trots att behörighet för detta saknades eller borde ha saknats. Det fanns bland annat möjlighet att ta del av känsliga personuppgifter och även andra särskilt skyddsvärda uppgifter, som skyddade personuppgifter och uppgifter om elevomdömen. (KRNS 7837-21)

Kammarrätten i Stockholm fastställde en sanktionsavgift om 11,3 miljoner kronor för Medhelp Sjukvårdsrådgivning AB, varav 7,8 miljoner kronor avsåg exponering av ljudfiler med inspelade telefonsamtal till 1177 mot internet. Bolaget bedömdes ha underlåtit att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå för uppgifterna i strid med artiklarna 5.1 f och 32.1 i dataskyddsförordningen. (KRNS 4058-22)

3.7 Ansvarsskyldighet

Artikel 5.2 i dataskyddsförordningen
Den personuppgiftsansvarige ska ansvara för och kunna visa att punkt 1 efterlevs *(ansvarsskyldighet)*.

Principen om ansvarsskyldighet innebär att vi inte bara ska följa de grundläggande principerna utan även måste vidta åtgärder för att säkerställa att vi följer dem samt visa att vi följer dem. Det kan vi göra på olika sätt, till exempel genom att tillhandahålla utbildningar om dataskydd för medarbetare och andra som behandlar personuppgifter åt oss, föra register över all behandling av personuppgifter som myndigheten ansvarar för och dokumentera behandlingar och risker. Principen om ansvarsskyldighet gäller även om behandlingen utförs av ett personuppgiftsbiträde.

4 Rättslig grund

I artikel 6 i dataskyddsförordningen finns en uttömmande uppräkning av när det är tillåtet (lagligt) att behandla personuppgifter (jämför principen om laglighet i avsnitt 3.1). För att en behandling av personuppgifter ska vara tillåten krävs att behandlingen sker med stöd av minst en av de grunder, så kallade *rättsliga grunder*, som räknas upp i artikeln.

De rättsliga grunderna är

- samtycke
- avtal med den registrerade
- rättslig förpliktelse
- skydd av grundläggande intressen
- uppgift av allmänt intresse eller led i myndighetsutövning
- intresseavvägning.

Försäkringskassans personuppgiftsbehandling grundas främst på *rättsliga förpliktelser, uppgifter av allmänt intresse* och *myndighetsutövning*.

Den rättsliga grunden *skydd av grundläggande intressen* tar sikte på personuppgiftsbehandling som är av avgörande betydelse för en registrerads eller annan fysisk persons liv och är inte aktuell att tillämpa på Försäkringskassan.

4.1 Nödvändighetskravet

När den registrerade har lämnat sitt samtycke till en behandling av personuppgifter krävs det inte att behandlingen är nödvändig, till skillnad från vad som gäller för övriga rättsliga grunder.

Att behandlingen ska vara nödvändig innebär att målet med behandlingen inte rimligen ska gå att uppnå på ett lika effektivt sätt genom andra medel som är mindre ingripande i de registrerades grundläggande fri- och rättigheter (EU-domstolens dom Latvijas Republikas Saeima, C-439/19, EU:C:2021:504, punkt 109 och 110).

Vi ska pröva kravet på nödvändighet tillsammans med principen om uppgiftsminimering (se EU-domstolens dom Meta Platforms m.fl. [Ett socialt nätverks användarvillkor], C-252/21, EU:C2023:537, punkt 109). Det innebär att när vi bedömer om behandlingen är nödvändig ska vi överväga om personuppgifterna som behandlas är adekvata och relevanta. Vi ska också säkerställa att behandlingen inte omfattar mer än vad som är nödvändigt med hänsyn till ändamålen för vilka uppgifterna samlas in. Läs mer om principen om uppgiftsminimering i avsnitt 3.3.

Kravet på nödvändighet ska inte läsas som att det ska vara omöjligt att uppnå syftet med behandlingen utan att personuppgifter behandlas. Kravet på nödvändighet innebär dock att personuppgifter inte får behandlas om syftet med behandlingen kan uppnås med andra medel, till exempel genom att anonymisera uppgifterna (prop. 2017/18:232 s. 117). I dagsläget anses det nästan alltid vara nödvändigt att behandla personuppgifter digitalt, eftersom en manuell informationshantering inte utgör ett realistiskt alternativ för varken myndigheter eller företag (se prop. 2017/18:105 s. 46 f. och EU-domstolens dom Huber mot Tyskland C-524/06, EU:C:2008:724, punkt 62).

4.2 De rättsliga grunderna

4.2.1 Samtycke

Artikel 6.1 a i dataskyddsförordningen
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.

Artikel 4.11 i dataskyddsförordningen
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.

Den rättsliga grunden samtycke innebär att den registrerade aktivt godkänner att den personuppgiftsansvariga behandlar hens personuppgifter. Samtycket kan lämnas skriftligt, muntligt eller genom konkludent handlande (att man genom sitt agerande visar att man har samtyckt). Eftersom den personuppgiftsansvariga måste kunna *visa* att den registrerade har samtyckt är det i de flesta fall bäst att inhämta skriftliga samtycken som enkelt kan förvaras och hittas.

Samtycke bör inte utgöra en giltig rättslig grund när det råder betydande ojämlikhet mellan den registrerade och den personuppgiftsansvariga, eftersom det påverkar möjligheterna att lämna ett frivilligt samtycke. Detta gäller särskilt om den personuppgiftsansvariga är en offentlig myndighet (skäl 43 till dataskyddsförordningen). Även i relationen mellan arbetsgivare och arbetstagare råder ofta betydande ojämlikhet mellan den registrerade och den personuppgiftsansvariga, vilket gör det svårt att uppfylla kravet på att ett samtycke ska lämnas frivilligt (EDPB:s riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679, s. 9).

Vi behandlar ofta personuppgifter om registrerade som befinner sig i underläge i förhållande till Försäkringskassan, till exempel inom förmånsverksamheten och den personaladministrativa verksamheten. Därför är det oftast olämpligt att använda samtycke som rättslig grund. Det kan dock vara aktuellt i vissa fall, till exempel vid publicering av fotografier på Fia, prenumeration på nyhetsbrev och anmälan till konferenser.

För att vi ska kunna använda oss av samtycke krävs att ett antal villkor är uppfyllda (artikel 7 i dataskyddsförordningen):

- Försäkringskassan ska i egenskap av personuppgiftsansvarig kunna visa att den registrerade har samtyckt till behandlingen.
- Det ska vara tydligt för den registrerade vad samtycket innebär och vilken behandling det omfattar. Samtycket får inte sammanblandas med andra frågor och vi måste presentera det i en begriplig och lätt tillgänglig form. När vi hämtar in samtycket ska vi använda ett klart och tydligt språk.
- Den registrerade ska kunna återkalla sitt samtycke när som helst – det ska vara lika lätt som att lämna det. Vi måste hålla samtycken ordnade och lätt tillgängliga så att det är enkelt att hantera en återkallelse. Det ska också vara möjligt att avbryta en behandling som den registrerade har samtyckt till, till exempel att avpublicera filmer på en webbplats eller att sluta använda en bild till en tryckt broschyr.

- Samtycket ska ha lämnats frivilligt. Det innebär att den registrerade inte får utsättas för några påtryckningar eller drabbas av negativa konsekvenser om hen väljer att inte samtycka.

4.2.2 Avtal

Artikel 6.1 b i dataskyddsförordningen
Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:

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.

Ett avtal kan vara rättslig grund för personuppgiftsbehandling under förutsättning att behandlingen är avgörande för att avtalets syfte ska gå att uppnå. Det räcker inte att behandlingen nämns i avtalet eller att den är till nytta för avtalet (EU-domstolens Mousse, C-394/23, ECLI:EU:C:2025:2, punkt 33 och 34).

Den registrerade måste själv vara part i avtalet. Vi kan exempelvis inte behandla personuppgifter om anställda hos en tjänsteleverantör med ett avtal mellan Försäkringskassan och tjänsteleverantören som rättslig grund.

Den som är personuppgiftsansvarig måste fullgöra avtalet för sin egen eller annans räkning, men behöver inte själv vara part i avtalet. Vi kan till exempel ha avtal som rättslig grund vid utbetalning av lön till anställda eftersom behandlingen av personuppgifter är nödvändig för att fullgöra villkoren i anställningsavtalen (jämför Brinnen, *Karnovs lagkommentar 105 till artikel 6 i dataskyddsförordningen*, JUNO Version 2026-07-01).

4.2.3 Rättslig förpliktelse

Artikel 6.1 c i dataskyddsförordningen
Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:

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

En rättslig förpliktelse är en skyldighet som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning (2 kap. 1 § dataskyddslagen). Det kan till exempel vara en skyldighet att lämna uppgifter eller att föra ett register. Det krävs inte att det finns en skyldighet att genomföra själva behandlingen av personuppgifterna, utan det räcker att behandlingen är nödvändig för att kunna fullgöra en rättslig förpliktelse.

Syftet med personuppgiftsbehandlingen måste framgå av den rättsliga förpliktelsen (artikel 6.3 i dataskyddsförordningen). Om förpliktelsen är alltför allmänt hållen och kan uppfyllas på olika sätt, kan den inte utgöra en rättslig grund för behandling av personuppgifter (SOU 2017:39 s. 114). Det ska vara möjligt för både den personuppgiftsansvariga och den registrerade att förstå varför behandlingen av personuppgifter ska ske (jämför prop. 2017/18:105 s. 54).

Ett exempel på en rättslig förpliktelse där syftet framgår är en uppgiftsskyldighet som anger att uppgifter i en viss situation ska lämnas till en annan aktör. Att Försäkringskassan enligt sin instruktion ska säkerställa att felaktiga utbetalningar inte görs och motverka bidragsbrott är ett exempel på en alltför allmänt hållen skyldighet som inte utgör en rättslig förpliktelse.

När en rättslig förpliktelse träffar en myndighet kan utförandet av förpliktelsen även vara ett allmänt intresse enligt artikel 6.1 e i dataskyddsförordningen.

4.2.4 Uppgift av allmänt intresse eller led i myndighetsutövning

Artikel 6.1 e i dataskyddsförordningen
Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:

e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

Den rättsliga grunden i artikel 6.1 e beskrivs ofta som tvådelad eftersom den innebär att behandlingen kan vara grundad antingen på en uppgift av allmänt intresse *eller* vara nödvändig som ett led i myndighetsutövning. Myndighetsutövning enligt lag eller annan författning får genomgående även anses vara ett allmänt intresse.

Försäkringskassan grundar en stor del av sin personuppgiftsbehandling på den rättsliga grunden i artikel 6.1 e. Enligt förarbetena till dataskyddslagen ska begreppet ”uppgift av allmänt intresse” ges en vid betydelse. Alla uppgifter som riksdag eller regering gett i uppdrag åt statliga myndigheter att utföra och den verksamhet som en statlig myndighet bedriver inom ramen för sin befogenhet är enligt regeringen av allmänt intresse (prop. 2017/18:105 s. 56 f.). De uppgifter som vi utför till följd av uppdrag i Försäkringskassans instruktion, regleringsbrev, specifika regeringsuppdrag, myndighetsförordningen (2007:515) och verksamhetsspecifika lagstiftningar, till exempel SFB, är generellt uppgifter av allmänt intresse (prop. 2023/24:29 s. 39). Även uppgifter som vi utför till följd av krav i annan lagstiftning, till exempel arbetsmiljölagen (1977:1160), får anses vara av allmänt intresse. Behandling av personuppgifter i samband med riskbedömningar gällande våld, hot eller otillåten påverkan med stöd av arbetsmiljölagen och Arbetsmiljöverkets föreskrifter grundas således på ett allmänt intresse.

En uppgift 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 (artikel 6.3 i dataskyddsförordningen och 2 kap. 2 § 1 dataskyddslagen) medan myndighetsutövning ska följa av lag eller annan författning (artikel 6.3 i dataskyddsförordningen och 2 kap. 2 § 2 dataskyddslagen). Den rättsliga grunden ska alltså vara rättsligt förankrad, vilket innebär att det måste finnas bestämmelser som medför ett behov av att behandla personuppgifter. Det måste däremot inte framgå av bestämmelsen att det krävs personuppgiftsbehandling. Även mer allmänt hållna uppdrag i Försäkringskassans instruktion, till exempel uppdraget i 2 § 3 att säkerställa att felaktiga utbetalningar inte görs och motverka bidragsbrott, kan tillgodose behovet av en rättslig förankring.

Administrativa åtgärder som indirekt krävs för att en myndighet ska fungera, får utföras om de anses nödvändiga för att myndigheten ska kunna utföra sitt uppdrag. Eftersom grunduppdraget är fastställt i nationell rätt anses i sin tur även de övriga administrativa behandlingarna nödvändiga och de har således rättslig grund i dataskyddsförordningens mening (prop. 2017/18:105 s. 60 ff.).

4.2.5 Intresseavvägning

Artikel 6.1 första stycket f och andra stycket i dataskyddsförordningen
Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:

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.

Den rättsliga grunden i artikel 6.1 f i dataskyddsförordningen kallas ofta förenklat för *intresseavvägning*. Den innebär att det kan vara tillåtet att behandla personuppgifter om den personuppgiftsansvarigas intresse av behandlingen väger tyngre än den enskildes intresse av skydd för sin personliga integritet.

Försäkringskassan får i egenskap av offentlig myndighet inte behandla personuppgifter med stöd av en intresseavvägning när vi fullgör våra uppgifter. Det innebär att vi inte får tillämpa intresseavvägning som rättslig grund för personuppgiftsbehandling vid bland annat handläggning av förmåner. Behandling av personuppgifter som en myndighet utför utanför den myndighetsspecifika verksamheten, till exempel inom personal- eller ekonomiadministration, skulle kunna ske med stöd av en intresseavvägning (SOU 2017:66 s. 193). Vi bör dock även i sådana fall i första hand behandla personuppgifter med stöd av andra rättsliga grunder, till exempel allmänt intresse.

4.3 Försäkringskassans kärnverksamhet

Lagstiftaren har bedömt att Försäkringskassans behandling av personuppgifter för de ändamål som anges i 114 kap. 8–10 §§ SFB sker antingen för en rättslig förpliktelse, en uppgift av allmänt intresse eller som ett led i myndighetsutövning. Vilken av grunderna som är tillämplig beror på skälet till att uppgifterna behöver behandlas. Den rättsliga grunden är i de allra flesta fall fastställd genom någon annan rättsakt än 114 kap. SFB, till exempel förmånsbestämmelserna i SFB eller vår instruktion (prop. 2017/18:171 s. 82 f. och prop. 2023/24:29 s. 39 f.).

Läs mer om ändamål i kärnverksamheten i avsnitt 5.1.

4.4 Särskilda statistikverksamheten

Inom Försäkringskassans särskilda statistikverksamhet behandlas personuppgifter för att ta fram olika typer av statistik. I verksamheten gäller, utöver dataskyddsförordningen, även bestämmelserna i lagen om den officiella statistiken och förordningen om den officiella statistiken. Den personuppgiftsbehandling som sker för att framställa statistik enligt lagen och förordningen sker som huvudregel för den rättsliga grunden allmänt intresse enligt artikel 6.1 e i dataskyddsförordningen (prop. 2017/18:107 s. 26).

4.5 Visselblåsarlagen

Vid rapportering av missförhållanden enligt visselblåsarlagen får personuppgifter bara behandlas om behandlingen är nödvändig för ett uppföljningsärende (7 kap. 1 § visselblåsarlagen). Den rättsliga grunden för sådan personuppgiftsbehandling är rättslig

förpliktelse eller allmänt intresse. Den rättsliga förpliktelsen respektive det allmänna intresset är fastställt genom visselblåsarlagen (prop. 2020/21:193 s. 175 f.).

5 Ändamål för behandling av personuppgifter

Vi får samla in personuppgifter endast om ett eller flera ändamål för behandlingen har fastställts vid insamlingstidpunkten. I vissa fall kan ändamål för behandlingen finnas fastställda i en registerförfattning. Detta kapitel beskriver de olika ändamålen i 114 kap. SFB, lagen om den officiella statistiken och visselblåsarlagen.

Om ändamål inte finns fastställda i en författning, måste Försäkringskassan själv fastställa ändamål. Det är fallet inom bland annat personaladministrativ verksamhet. Läs mer om detta i avsnitt 3.2.

5.1 Ändamål i kärnverksamheten

I 114 kap. SFB finns det en uppräkning av de ändamål för vilka Försäkringskassan får behandla personuppgifter inom kärnverksamheten. Det handlar dels om primära ändamål som gäller vår interna verksamhet, dels sekundära ändamål som gäller behov som finns utanför Försäkringskassan.

Flera av ändamålen är generellt formulerade. Vi får till exempel behandla personuppgifter om det är nödvändigt för att handlägga ärenden. I själva verket kan personuppgifter behandlas för mängder av olika syften inom ramen för handläggningen av ett ärende, även om det övergripande ändamålet är att handlägga ärendet. Vi kan behöva formulera mer preciserade ändamål för specifika behandlingar av personuppgifter för att uppfylla kravet på tydliga ändamål (jfr prop. 2023/24:29 s. 33).

5.1.1 Tillgodose behov av underlag

114 kap. 8 § 1 SFB
Försäkringskassan och Pensionsmyndigheten får behandla personuppgifter om det är nödvändigt för att

1. tillgodose behovet av det underlag som krävs för att den registrerades eller någon annans rättigheter eller skyldigheter i fråga om förmåner och ersättningar ska kunna bedömas eller fastställas,

Ändamålet i 114 kap. 8 § 1 SFB tar sikte på behandling av sådana personuppgifter som Försäkringskassan inhämtar eller tar del av innan eller utan att ett ärende inleds. Vi behöver till exempel ha tillgång till uppdaterade folkbokföringsuppgifter och andra adressuppgifter för en effektiv administration. Det kommer också in läkarintyg från vården och uppgifter om sjuklön från arbetsgivare, utan att den försäkrade först har gjort en ansökan om ersättning. Därutöver lämnar myndigheter och andra aktörer uppgifter på eget initiativ och till följd av underrättelseskyldigheter.

5.1.2 Informera om förmåner och ersättningar

114 kap. 8 § 2 SFB
Försäkringskassan och Pensionsmyndigheten får behandla personuppgifter om det är nödvändigt för att

2. informera om förmåner och ersättningar,

Försäkringskassan har i uppdrag att informera om socialförsäkringen och dess förmåner

och ersättningar. Uppdraget förutsätter behandling av personuppgifter, i första hand uppgifter om namn och adresser. Det kan även vara aktuellt att genom olika kriterier göra urval av mottagare av informationen, vilket förutsätter fler uppgifter än enbart kontaktuppgifter.

Information kan skickas ut inom ramen för ett ärende, vilket då sker med stöd av ändamålet som avser handläggning av ärenden, men ofta kan det vara fråga om mer allmänt riktad information. Vi skickar till exempel information till blivande föräldrar om föräldrapenning och information om bland annat regelförändringar till personer som kan tänkas bli berörda.

5.1.3 Handlägga ärenden

114 kap. 8 § 3 SFB
Försäkringskassan och Pensionsmyndigheten får behandla personuppgifter om det är nödvändigt för att

3. handlägga ärenden,

Handläggning av ärenden om förmåner och ersättningar är den centrala delen av Försäkringskassans kärnverksamhet. Inom handläggningen behandlas stora mängder personuppgifter, vilket är en förutsättning för att vi ska kunna fullgöra våra uppgifter.

I förvaltningslagen innefattar uttrycket ”handläggning av ärenden” alla åtgärder som en myndighet vidtar från att ett ärende inleds tills det avslutas (prop. 2016/17:180 s. 286). Uttrycket ärende definieras inte i förvaltningslagen men enligt förarbetena avslutas ett ärende regelmässigt genom ett uttalande från myndighetens sida som är avsett att få faktiska verkningar för en mottagare i det enskilda fallet, det vill säga ett beslut. Regeringen har i förarbetena till dataskyddslagen uttalat att uttrycket ”handläggningen av ett ärende” i 3 kap. 3 § 2 dataskyddslagen ska tolkas på samma sätt som enligt förvaltningslagen (prop. 2017/18:105 s. 194).

I förarbetena till domstolsdatalagen (2015:728) har regeringen ansett att ett ändamål som avser handläggning av mål och ärenden inte ska tolkas alltför snävt. Bedömningen av om en viss behandling är nödvändig ska göras i förhållande till mål- och ärendehandläggningen i stort och inte i förhållande till handläggningen av ett specifikt mål eller ärende (prop. 2014/15:148 s. 39 f.).

Ändamålet att handlägga ärenden bör omfatta behandling av personuppgifter till exempel i samband med att vi tar emot och inhämtar handlingar och uppgifter, diarieför och registrerar, bereder ärendet, vidtar utredande åtgärder, kommunicerar, kontaktar kollegor inom samma myndighet med anledning av ärendet, hanterar praxis, upprättar, meddelar och verkställer beslutet samt betalar ut förmånen eller ersättningen. Även sådan behandling av personuppgifter som sker efter att ärendet har avslutats bör kunna anses ske för ändamålet att handlägga ärenden, om de åtgärder som vidtas anknyter till ärendet. Det kan handla om till exempel impulser, indexomräkningar, uppräkningar och avräkningar. En omprövning, ett överklagande, en kontrollutredning, ett återkrav och liknande hanteras i nya ärenden, men innan nya ärenden inleds – och när det föregående ärendet är avslutat – kan åtgärder vidtas som syftar till att bedöma om ett sådant nytt ärende ska inledas. Även personuppgiftsbehandling med anledning av sådana åtgärder får anses ske för ändamålet att handlägga ärenden. Personuppgifter som ska gallras sparas under en viss tid innan de gallras. Den behandling som sker genom att uppgifterna sparas tills de gallras sker för ändamålet att handlägga ärenden.

Personuppgifter som samlats in för ett visst ärende kan i vissa fall behöva behandlas i ett annat ärende som rör samma person eller i ett ärende som rör en annan person, men där den registrerade förekommer som till exempel anhörig. Det kan också komma in handlingar i ett ärende som saknar omedelbar betydelse för handläggningen. Ändamålet handläggning av ärenden bör ge utrymme att behandla personuppgifter i inkomna handlingar utan att det i det enskilda fallet sker någon bedömning av hur relevant uppgiften är för ett visst mål eller ärende (jämför prop. 2014/15:148 s. 40).

Ändamålet att handlägga ärenden är tillämpligt i olika typer av ärenden. Framför allt aktualiseras det vid prövning av rätt till förmåner eller ersättningar, men det ska också tillämpas vid till exempel omprövning, processföring i domstol, skadeståndsärenden, registervårdsärenden och handläggning av remisser från JO, JK och DO om ärendena behandlar frågor som rör sådan behandling av personuppgifter som omfattas av tillämpningsområdet för 114 kap. SFB.

5.1.4 Vidta kontrollåtgärder

114 kap. 8 § 4 SFB
Försäkringskassan och Pensionsmyndigheten får behandla personuppgifter om det är nödvändigt för att

4. vidta kontrollåtgärder som syftar till att förebygga, förhindra och upptäcka felaktiga utbetalningar och bidragsbrott,

Med uttrycket kontrollåtgärder avses åtgärder som innebär att övervaka, granska eller undersöka Försäkringskassans handläggning och utbetalningar av förmåner och ersättningar. Syftet med kontrollerna ska vara att förebygga, förhindra och upptäcka felaktiga utbetalningar och bidragsbrott.

Enligt förarbetena (prop. 2023/24:29 s. 37 och 98 f.) kan det till exempel röra sig om kontrollåtgärder i form av:

- behandling av personuppgifter genom analyser av uppgifter, för att
  - utveckla nya och effektivare metoder för kontroll, till exempel maskinella riskbaserade analyser och urval
  - utveckla och träna modeller
  - identifiera ärenden som ska ingå i ett avsett urval
- kontroller av det statliga tandvårdsstödet som sker genom systematisk bearbetning av elektroniska data, där vi särskilt ska kontrollera uppgifter som lämnas i samband med behandling och som av någon anledning avviker från vad som kan anses normalt eller som vi bör uppmärksamma av andra skäl (prop. 2007/08:49 s. 98)
- insamlande av uppgifter och utförande av de systematiska kontroller av utnyttjande av assistansersättning som Skatteverkets uppgiftsskyldighet enligt 110 kap. 34 a § SFB är tänkt att möjliggöra
- behandling av personuppgifter som sker i anslutning till att uppgifter lämnas till och från Försäkringskassan med stöd av till exempel
  - lagen (2008:206) om underrättelseskyldighet vid felaktiga utbetalningar från välfärdssystemen
  - lagen (2016:774) om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet
  - behandling av personuppgifter med anledning av en polisanmälan.

Ändamålet som avser kontrollåtgärder bör även vara tillämpligt vid behandling av

personuppgifter som sker i anslutning till att uppgifter lämnas till och från Försäkringskassan med stöd av till exempel:

- lagen (2024:307) om uppgiftsskyldighet för att motverka felaktiga utbetalningar från välfärdssystemen samt fusk, regelöverträdelser och brottslighet i arbetslivet (LUFFA)
- lagen (2025:170) om skyldighet att lämna uppgifter till de brottsbekämpande myndigheterna
- 10 kap. 15 a § OSL.

När personuppgifter behandlas för olika kontrolländamål inom ramen för ärende-handläggningen, kan behandlingen i de flesta fall ske med stöd av ändamålet att handlägga ärenden. Det gäller i både ordinarie handläggning och kontrollutredningsärenden.

5.1.5 Verksamhetsplanering, resultatstyrning, resultatuppföljning, resultatredovisning, utvärdering eller tillsyn

114 kap. 8 § 5 och 6 SFB
Försäkringskassan och Pensionsmyndigheten får behandla personuppgifter om det är nödvändigt för att

5. planera sina respektive verksamheter,

6. inom sina respektive verksamheter genomföra resultatstyrning, resultatuppföljning, resultatredovisning, utvärdering eller tillsyn,

Ändamålen i 114 kap. 8 § 5 och 6 SFB ger Försäkringskassan stöd för att behandla personuppgifter i syfte att dels planera verksamheten, dels genomföra resultatstyrning, resultatuppföljning, resultatredovisning, utvärdering eller tillsyn. Det kan enligt förarbetena (prop. 2002/03:135 s. 65) till exempel handla om att

- följa ärendemängder och ärendens status i syfte att leda, fördela och följa upp handläggarnas arbete
- analysera utvecklingen inom de olika förmånsslagen
- analysera utvecklingen av Försäkringskassans administration av förmånerna
- utvärdera effekterna för individ och samhälle av utvecklingen inom socialförsäkringen och anslutande bidragssystem
- utveckla prognosmodeller samt ta fram prognoser för och analyser av utgifterna för de socialförsäkrings- och bidragssystem som Försäkringskassan administrerar.

5.1.6 Framställa statistik

114 kap. 8 § 7 SFB
Försäkringskassan och Pensionsmyndigheten får behandla personuppgifter om det är nödvändigt för att

7. framställa statistik i fråga om verksamhet enligt 3–6.

Vi får behandla personuppgifter om det är nödvändigt för att framställa statistik som

gäller handläggningen av ärenden, kontrollåtgärder och verksamhetsplanering, resultatstyrning, resultatuppföljning, resultatredovisning, utvärdering eller tillsyn. Det krävs för att vi ska kunna utföra vårt uppdrag att följa, analysera och förmedla socialförsäkringssystemets utveckling och effekter för enskilda och samhälle, men också för bland annat verksamhetsuppföljning och planering samt med anledning av externa beställningar från regeringen, utredningar och forskare.

Den behandling av personuppgifter som vi utför som en del av uppdraget att ansvara för den officiella statistiken omfattas inte av tillämpningsområdet för 114 kap. SFB. För sådan verksamhet finns särskilda bestämmelser om behandling av personuppgifter i lagen om den officiella statistiken och anslutande författningar. I 114 kap. 4 § SFB anges därför att det i fråga om behandling av personuppgifter inom ramen för den officiella statistiken finns särskilda bestämmelser i lagen om den officiella statistiken och i författningar som ansluter till den lagen.

5.1.7 Testverksamhet

Förvaltning, utveckling och underhåll av Försäkringskassans it-system förutsätter ofta testning. Testning kan ofta göras med hjälp av avidentifierade uppgifter som saknar koppling till individer. Sådana uppgifter är inte personuppgifter och omfattas därmed inte av dataskyddslagstiftningens krav. Det är dock viktigt att vara observant på att uppgifter kan vara personuppgifter genom indirekt identifiering även om de saknar koppling till namn eller personnummer (läs mer i avsnitt 1.2.1).

I vissa fall kan tester med personuppgifter vara en förutsättning för att personuppgifter ska behandlas på ett korrekt sätt i den faktiska verksamheten. Testverksamhet regleras vanligen inte som ett särskilt ändamål i registerförfattningar. I stället anses testverksamhet vara så nära knuten till övrig verksamhet att behandlingen av personuppgifter sker med stöd av något av ändamålen i 114 kap. 8 § SFB eller efter en bedömning enligt finalitetsprincipen i 114 kap. 10 § SFB (jämför prop. 2023/24:29 s. 45 f.).

Försäkringskassan har i egenskap av personuppgiftsansvarig ansvar för att vidta åtgärder för att säkerställa säkerheten i de tekniska systemen. Vi ska bland annat genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen (artikel 24.1). Vi ska också vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Det ska göras med beaktande av den senaste utvecklingen, kostnaderna för genomförande och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter (artikel 32.1). En sådan åtgärd ska, när det är lämpligt, vara ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet. Redan inom ramen för dataskyddsförordningen ställs alltså krav på åtgärder som avser testverksamhet.

När vi genom tester säkerställer att Försäkringskassan har väl fungerande it-system för att i förlängningen kunna fullgöra de åligganden som vilar på oss i vår verksamhet, handlar det om administrativa åtgärder som är nödvändiga för myndigheters förvaltning och funktion (prop. 2019/20:113 s. 19 f.). Behandling av personuppgifter som utförs som ett led i sådana administrativa åtgärder som är nödvändiga för myndigheters förvaltning och funktion är rättsligt grundad i den mening som avses i artikel 6 i dataskyddsförordningen (se avsnitt 4.2.4).

Utöver att säkerställa att det finns en tillämplig rättslig grund måste vi alltid bedöma om testningen är nödvändig för att Försäkringskassan ska kunna utföra sin verksamhet på det effektiva sätt som krävs enligt myndighetsförordningen. Vi måste också fastställa ett

tillräckligt preciserat ändamål och utföra testverksamheten i enlighet med övriga bestämmelser om dataskydd.

Läs mer
Skillnaden mellan testverksamhet och mer innovativ it-utveckling beskrivs i Försäkringskassans vägledning (2024:3) Digitalisering på Försäkringskassan.

5.1.8 Utlämnande av uppgifter

114 kap. 9 § SFB
Personuppgifter som behandlas för ändamål som anges i 8 § får behandlas av Försäkringskassan och Pensionsmyndigheten även för att fullgöra uppgiftslämnande som

1. sker i överensstämmelse med lag eller förordning, eller

2. följer av unionsrätten, åtaganden i samarbetet inom Europeiska ekonomiska samarbetsområdet eller avtal om social trygghet eller utgivande av sjukvårdsförmåner som Sverige ingått med andra stater.

Vi får lämna ut personuppgifter som har samlats in för Försäkringskassans interna verksamhet under förutsättning att det sker i enlighet med bestämmelser i lag, förordning eller vissa internationella åtaganden.

Med uppgiftslämnande som sker i överensstämmelse med lag eller förordning menas att uppgifter lämnas med stöd av bestämmelser som antingen innebär en skyldighet att lämna ut uppgifter eller tillåter att så sker. Det kan till exempel röra sig om en sådan uttrycklig uppgiftsskyldighet som avses i 10 kap. 28 § OSL eller om uppgiftslämnande i syfte att fullgöra serviceskyldigheten enligt förvaltningslagen. Uppgiftslämnandet kan även ske med stöd av 6 kap. 5 § OSL som innebär att vi är skyldiga att på begäran av en annan myndighet lämna ut en uppgift som vi förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång. (Prop. 2023/24:29 s. 47)

Läs mer
Läs mer om 6 kap. 5 § och 10 kap. 28 § OSL i Försäkringskassans vägledning (2001:3) *Offentlighet, sekretess och utlämnande av handlingar och uppgifter*.

Serviceskyldigheten enligt förvaltningslagen beskrivs i Försäkringskassans vägledning (2004:7)) *Förvaltningsrätt i praktiken.*

Delar av den personuppgiftsbehandling som sker inom ramen för EU-samarbetet är reglerad i EU-förordningar som gäller som svensk lag. Enligt regeringen kan det dock inte uteslutas att nödvändigt internationellt uppgiftslämnande inte kan ske i överensstämmelse med svensk lag eller förordning. Det finns därför ett särskilt ändamål i 114 kap. 9 § 2 SFB som reglerar detta. (Prop. 2023/24:29 s. 48 f.)

När Försäkringskassan samlar in personuppgifter i kärnverksamheten behandlas personuppgifterna med stöd av något av de primära ändamålen i 114 kap. 8 § SFB, till exempel för handläggningen av ett socialförsäkringsärende. Försäkringskassan får inte

samla in personuppgifter inom kärnverksamheten enbart i syfte att lämna ut dem. Det framgår av 114 kap. 9 § SFB, som endast tillåter behandling av personuppgifter som redan behandlas för ändamål som anges i 114 kap. 8 § SFB.

5.1.9 Behandling av personuppgifter med stöd av finalitetsprincipen

114 kap. 10 § SFB
Personuppgifter som behandlas enligt 8 eller 9 § får behandlas även för andra ändamål, under förutsättning att uppgifterna inte behandlas på ett sätt som är oförenligt med det ändamål för vilket uppgifterna samlades in.

Bestämmelsen i 114 kap. 10 § SFB ger uttryck för den så kallade finalitetsprincipen och infördes ursprungligen i syfte att tydliggöra att de i övrigt angivna ändamålen inte ska ses som uttömmande (prop. 2002/03:135 s. 131 f.). Senare har det av tydlighetsskäl ansetts finnas behov av en hänvisning till finalitetsprincipen (prop. 2017/18:171 s. 89 och 192 och prop. 2023/24:29 s. 49 f.).

Finalitetsprincipen kan enligt förarbetena inte tillämpas utan avvägningar som i praktiken innebär att de nya ändamålen kommer att behöva ligga mycket nära de ursprungliga ändamålen eller kunna ses som en förlängning av dem (prop. 2023/24:29 s. 50). Läs mer om tillämpningen av finalitetsprincipen i avsnitt 3.2.

Särskilda begränsningar gäller vid behandling av känsliga personuppgifter med stöd av finalitetsprincipen (se avsnitt 6.6.1).

Försäkringskassan har i ett rättsligt ställningstagande uttalat att bestämmelsen i 114 kap. 10 § SFB ska tolkas som att personuppgifter som behandlas enligt 114 kap. 8 eller 9 § SFB får behandlas även för ändamål utanför tillämpningsområdet för 114 kap. SFB (RS 2025:04). Utrymmet för vidarebehandling utanför tillämpningsområdet för 114 kap. SFB är enligt ställningstagandet mycket begränsat och förutsätter en noggrann prövning.

5.2 Ändamål i statistikverksamheten

14 § första stycket lagen om den officiella statistiken
En statistikansvarig myndighet får behandla personuppgifter för framställning av statistik om inte annat följer av 15 §. […]

Försäkringskassan får i egenskap av statistikansvarig myndighet behandla personuppgifter för framställning av statistik. Det bör omfatta all verksamhet i samband med insamling, lagring, bearbetning och analys som är nödvändig för att sammanställa statistik.

När vi behandlar personuppgifter för statistikändamål behöver vi oftast formulera mer preciserade ändamål för specifika behandlingar av personuppgifter för att uppfylla kravet på tydliga ändamål (jfr avsnitt 3.2).

5.3 Ändamål i visselblåsarlagen

Primära ändamål

7 kap. 3 § visselblåsarlagen
Personuppgifter får behandlas bara om behandlingen är nödvändig för ett uppföljningsärende.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om begränsningar av ändamålen och om begränsningar av vilka personuppgifter som får behandlas för ett visst ändamål.

Vid rapportering av missförhållanden enligt visselblåsarlagen får personuppgifter bara behandlas om behandlingen är nödvändig för ett uppföljningsärende. Behandling av personuppgifter för ändamålet innefattar enligt förarbetena (prop. 2020/21:193 s. 184) att:

- ta emot rapporter och ha kontakt med den rapporterande personen
- dokumentera rapporter, vilket kan omfatta skriftlig dokumentation eller inspelning av muntlig information
- bekräfta mottagandet av en rapport till den rapporterande personen
- vidta åtgärder för att bedöma riktigheten i de påståenden som framställs i rapporterna, vilket kan inkludera kontakter med andra personer i syfte att bekräfta eller vederlägga påståendena
- återkoppla till den rapporterande personen om den utförda utredningen och de slutsatser som har dragits av utredningen.

Det har inte meddelats några föreskrifter om begränsningar av ändamålen eller om begränsningar av vilka personuppgifter som får behandlas enligt visselblåsarlagen. Det är dock viktigt att beakta de grundläggande principerna enligt artikel 5 i dataskyddsförordningen.

Sekundära ändamål

7 kap. 4 § visselblåsarlagen
Personuppgifter som behandlas för ändamålet i 3 § får också behandlas för att fullgöra ett uppgiftslämnande som

1. är nödvändigt för att åtgärder ska kunna vidtas med anledning av det som har framkommit i ett ärende,

2. är nödvändigt för att rapporter ska kunna användas som bevisning i rättsliga förfaranden, eller

3. sker i överensstämmelse med lag eller förordning.

Personuppgifter som behandlas i ett uppföljningsärende enligt visselblåsarlagen får under vissa omständigheter behandlas för att lämnas ut från Försäkringskassan.

Vi får lämna ut personuppgifter om utlämnandet är nödvändigt för att åtgärder ska kunna vidtas med anledning av det som har kommit fram i ett ärende. Det kan handla om åtgärder som behöver vidtas av en ledningsfunktion, rättsfunktion eller personalfunktion

inom verksamheten. Vi får också lämna ut personuppgifter om det är nödvändigt för att rapporter ska kunna användas som bevisning i rättsliga förfaranden. De förfaranden som kan vara aktuella är framför allt tvister enligt visselblåsarlagen, arbetsrättsliga tvister om skiljande från anställningen och brottmålsförfaranden rörande till exempel ärekränkning. Personuppgifter får dessutom lämnas ut om det sker i överensstämmelse med lag eller förordning, till exempel för att uppfylla krav enligt OSL (prop. 2020/21:193 s. 300).

Finalitetsprincipen

7 kap. 5 § visselblåsarlagen

Personuppgifter som behandlas för ändamålet i 3 § får behandlas även för andra ändamål, under förutsättning att uppgifterna inte behandlas på ett sätt som är oförenligt med det ändamål för vilket uppgifterna samlades in.

Bestämmelsen i 7 kap. 5 § visselblåsarlagen ger uttryck för finalitetsprincipen. Bestämmelsen tydliggör att finalitetsprincipen gäller vid behandling av personuppgifter enligt 7 kap. visselblåsarlagen. Läs mer om finalitetsprincipen i avsnitt 3.2.

6 Känsliga personuppgifter och andra särskilt skyddsvärda personuppgifter

Vissa personuppgifter anses så skyddsvärda att de omfattas av särskilda begränsningar i dataskyddsförordningen och övrig dataskyddsreglering. Det handlar om dels känsliga personuppgifter, dels andra särskilt skyddsvärda personuppgifter.

6.1 Vad är känsliga personuppgifter?

Artikel 9.1 i dataskyddsförordningen
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.

3 kap. 1 § dataskyddslagen
Med känsliga personuppgifter avses i denna lag sådana uppgifter som avses i artikel 9.1 i EU:s dataskyddsförordning.

Vissa särskilda kategorier av personuppgifter är enligt dataskyddsförordningen som huvudregel inte tillåtna att behandla. Det handlar om:

- uppgifter som avslöjar ras eller etniskt ursprung
- uppgifter som avslöjar politiska åsikter
- uppgifter som avslöjar religiös eller filosofisk övertygelse
- uppgifter som avslöjar medlemskap i fackförening
- genetiska uppgifter
- biometriska uppgifter för att entydigt identifiera en fysisk person
- uppgifter om hälsa
- uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Dessa särskilda kategorier av uppgifter kallas känsliga personuppgifter.

Begreppet känsliga personuppgifter ska ges en vid tolkning. Även uppgifter som indirekt avslöjar uppgifter om hälsa eller en fysisk persons sexualliv eller sexuella läggning har ansetts vara känsliga personuppgifter.

Rättsfall
EU-domstolen har ansett att uppgifter som indirekt – genom en intellektuell jämförelse eller slutledning – avslöjar uppgifter om en fysisk persons sexuella läggning ska anses vara känsliga personuppgifter. I det aktuella målet rörde frågan uppgifter om bland annat make/maka, sambo eller partner (EU-domstolens dom Vyriausioji tarnybinės etikos komisija, C-184/20, EU:C:2022:601, punkt 123–127).

Vissa kategorier av känsliga personuppgifter är vanliga hos Försäkringskassan. Det handlar framför allt om personuppgifter om hälsa, men även vissa andra kategorier av

känsliga personuppgifter aktualiseras emellanåt. I det här avsnittet listas de kategorier som oftast väcker frågor inom vår verksamhet.

Uppgifter om hälsa

Personuppgifter om hälsa är ett vitt begrepp som täcker in alla uppgifter som avslöjar något om en persons tidigare, nuvarande eller framtida fysiska eller psykiska hälsotillstånd (skäl 35 och artikel 4.15 i dataskyddsförordningen). Det kan röra sig om uppgifter som beskriver ett hälsotillstånd, till exempel uppgifter om diagnos eller funktionsnedsättning. Även uppgifter som mer indirekt säger något om en viss persons hälsotillstånd kan vara personuppgifter om hälsa. Att någon har ansökt om, beviljats eller fått avslag på en ansökan om vissa sjukförsäkringsförmåner kan avslöja något om personens tidigare, nuvarande eller framtida hälsotillstånd. Sådana uppgifter kan därför utgöra känsliga personuppgifter om hälsa (prop. 2023/24:29 s. 67). Även uppgifter om nedsatt arbetsförmåga, om vårdmottagningar där den enskilde sökt vård, utförda behandlingsåtgärder när det handlar om tandvårdsersättning och ersättningsperioder kan vara känsliga personuppgifter om hälsa (prop. 2023/24:29 s. 54).

Om en personuppgiftsbehandling till sin karaktär är sådan att den kan avslöja information om en fysisk persons hälsotillstånd, ska uppgifterna hanteras som känsliga personuppgifter. Det gäller även om det inte med full säkerhet kan fastställas vem vissa av uppgifterna avser.

Rättsfall

EU-domstolen har ansett att information som ett apoteksföretags kunder lämnar i samband med att de beställer apoteksexklusiva receptfria läkemedel på en e-handelsplattform utgör hälsouppgifter. Det gäller även om det endast med viss grad av sannolikhet och inte med full säkerhet kan fastställas att dessa läkemedel är avsedda för kunderna som beställt dem. (EU-domstolens dom Lindenapotheke, C-21/23, EU:C:2024:846, punkt 90)

Vi bör alltid hantera uppgifter om ärenden om socialförsäkringsförmåner som känsliga personuppgifter, om uppgiften kan avslöja något om en persons hälsa. Det innefattar bland annat uppgifter om ärende-id.

Uppgifter om sexualliv eller sexuell läggning

Alla uppgifter som direkt eller indirekt kan avslöja något om en persons sexualliv eller sexuella läggning är känsliga personuppgifter. I sammanhanget är det viktigt att komma ihåg att alla slags sexuella läggningar omfattas.

En uppgift om att någon är gift eller sambo med en viss person kan avslöja båda personernas sexuella läggning (EU-domstolens dom Vyriausioji tarnybinės etikos komisija, C-184/20, EU:C:2022:601, punkt 100).

Uppgifter som avslöjar etniskt ursprung

En uppgift om medborgarskap, nationalitet eller vilket land någon kommer ifrån avslöjar normalt inte etniskt ursprung (prop. 2009/10:85 s. 325). Däremot kan passhandlingar som innehåller bild i förening med namn och medborgarskap avslöja etnicitet (prop. 2008/09:70 s. 142). Uppgifter om namn och språkkunskaper kan tillsammans utgöra indirekta upplysningar om en persons etniska ursprung (SOU 2017:57 s. 347).

I dataskyddsförordningen används även ordet ”ras”. Det innebär inte att EU godtar teorier om att det skulle finnas skilda människoraser (skäl 51 till dataskyddsförordningen).

Uppgifter som avslöjar medlemskap i fackförening

En mejladress som innehåller ett fackföreningsnamn skulle kunna avslöja en persons fackföreningstillhörighet (jämför SOU 2017:57 s. 346).

Enligt regeringen är medlemskap i en viss a-kassa inte i sig en känslig personuppgift eftersom a-kassorna är självständiga i förhållande till arbetstagarorganisationerna (prop. 2009/10:7 s. 24).

6.2 När får känsliga personuppgifter behandlas?

All behandling av personuppgifter förutsätter att det finns en tillämplig rättslig grund (avsnitt 4). Övriga bestämmelser i dataskyddsförordningen och eventuellt tillämplig registerförfattning ska också vara uppfyllda. För att det ska vara tillåtet att behandla känsliga personuppgifter krävs dessutom att något av de undantag som regleras i artikel 9.2 i dataskyddsförordningen är tillämpligt. Flera undantag kan vara tillämpliga samtidigt (prop. 2017/18:105 s. 80).

Undantagen ska enligt EU-domstolen tolkas restriktivt (EU-domstolens dom Meta Platforms m.fl., C-252/21, EU:C:2023:537, punkt 76).

Följande avsitt beskriver de undantag som främst kan aktualiseras för Försäkringskassan. De flesta undantagen förutsätter att behandlingen av personuppgifter är nödvändig. Nödvändighetsbegreppet beskrivs i avsnitt 4.1.

6.3 Behandling med stöd av samtycke

Artikel 9.2 a i dataskyddsförordningen

Punkt 1 ska inte tillämpas om något av följande gäller:

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.

Det kan vara tillåtet att behandla känsliga personuppgifter om den registrerade uttryckligen har lämnat sitt samtycke till behandlingen för ett eller flera specifika ändamål. Myndigheter bör dock som utgångspunkt inte använda sig av samtycke (skäl 43 till dataskyddsförordningen).

Ett samtycke till behandling av känsliga personuppgifter är fristående från den rättsliga grunden samtycke enligt artikel 6.1 i dataskyddsförordningen. Den rättsliga grunden för behandlingen behöver alltså inte vara samtycke även om känsliga personuppgifter behandlas med stöd av samtycke.

Ett samtycke enligt artikel 9.2 a i dataskyddsförordningen ska uppfylla samma krav som ett samtycke enligt artikel 6.1. Det innebär att samtycket ska vara en frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, godtar behandling av personuppgifter som rör hen (artikel 4.11 i dataskyddsförordningen). Den personuppgiftsansvariga ska kunna visa att den registrerade har samtyckt till behandlingen av sina personuppgifter (artikel 7.1 i dataskyddsförordningen) och innan den registrerade lämnar sitt samtycke ska hen få information om rätten att återkalla ett lämnat samtycke (artikel 7.3 i dataskyddsförordningen). Läs mer om i vilka situationer Försäkringskassan kan använda samtycke och vad som krävs för att ett samtycke ska vara giltigt i avsnitt 4.2.1.

6.4 Behandling inom arbetsrätten

Artikel 9.2 b i dataskyddsförordningen

Punkt 1 ska inte tillämpas om något av följande gäller:

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.

3 kap. 2 § dataskyddslagen

Känsliga personuppgifter får behandlas med stöd av artikel 9.2 b i EU:s dataskyddsförordning, om behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och inom områdena social trygghet och socialt skydd.

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

Bestämmelsen i artikel 9.2 b i dataskyddsförordningen gör det möjligt att behandla känsliga personuppgifter när det är nödvändigt för att arbetsgivare, arbetstagare, fackliga organisationer och arbetsgivarorganisationer ska kunna fullgöra sina skyldigheter eller utöva sina rättigheter med koppling till arbetslivet. Bestämmelsen kan därmed tillämpas vid behandling av personuppgifter som Försäkringskassan i egenskap av arbetsgivare utför som en följd av bland annat överenskommelser i kollektivavtal och bestämmelser i diskrimineringslagen (2008:567), lagen (1991:1047) om sjuklön och SFB, till exempel i samband med en arbetstagares sjukdom och rehabilitering. Även de fackliga organisationerna får behandla känsliga personuppgifter med stöd av artikel 9.2 b i dataskyddsförordningen. (Jämför prop. 2017/18:105 s. 78.)

För att det ska vara tillåtet att behandla känsliga personuppgifter för att fullgöra skyldigheter eller utöva rättigheter inom arbetsrätten krävs

- att behandlingen är tillåten enligt svensk rätt eller kollektivavtal, och
- att det rättsliga stödet innehåller bestämmelser om lämpliga skyddsåtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

För att möjliggöra sådan behandling och tillgodose kravet på skyddsåtgärder har en kompletterande bestämmelse införts i 3 kap. 2 § dataskyddslagen. Skyddsåtgärden enligt dataskyddslagen består i att känsliga personuppgifter som behandlas med stöd av 9.2 b i dataskyddsförordningen får lämnas ut till tredje part bara om det finns en skyldighet för den personuppgiftsansvariga att göra det eller den registrerade har samtyckt till utlämnandet. Skyldigheten att lämna ut personuppgifter ska följa av lagstiftning, myndighetsbeslut eller avtal (prop. 2017/18:105 s. 193).

6.5 Behandling vid rättsliga anspråk

Artikel 9.2 f i dataskyddsförordningen
Punkt 1 ska inte tillämpas om något av följande gäller:

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

Känsliga personuppgifter kan få behandlas om behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk. Det är inte helt klart vad som menas med rättsliga anspråk. Förmodligen är det sådana anspråk som man kan föra talan i domstol om (Öman, *Dataskyddsförordningen [GDPR] m.m. En kommentar*, JUNO Version 4, kommentaren till artikel 9). Själva behandlingen av de känsliga personuppgifterna behöver inte gå ut på att fastställa, göra gällande eller försvara det rättsliga anspråket. Det räcker att behandlingen är nödvändig för att anspråket ska kunna fastställas, göras gällande eller försvaras.

Försäkringskassan kan oftast utföra nödvändig behandling av känsliga personuppgifter av hänsyn till ett viktigt allmänt intresse (se följande avsnitt). Det är därför tveksamt om undantaget för rättsliga anspråk kan bli aktuellt för oss. Undantaget skulle dock kunna tillämpas med anledning av exempelvis en stämningsansökan eller i en avtalssituation.

6.6 Behandling av hänsyn till ett viktigt allmänt intresse

Artikel 9.2 g i dataskyddsförordningen
Punkt 1 ska inte tillämpas om något av följande gäller:

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.

3 kap. 3 § dataskyddslagen
Känsliga personuppgifter får behandlas av en myndighet med stöd av artikel 9.2 g i EU:s dataskyddsförordning

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

2. om behandlingen är nödvändig för handläggningen av ett ärende, eller

3. i annat fall, om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

Vid behandling som sker enbart med stöd av första stycket är det förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter.

[…]

Till skillnad från den rättsliga grunden allmänt intresse i artikel 6.1 e i dataskydds-förordningen, gäller undantaget i artikel 9.2 g ett *viktigt* allmänt intresse. Det är inte helt

klart vad som är skillnaden mellan de två begreppen. Regeringen har uttalat att det torde stå klart att verksamhet som innefattar myndighetsutövning utgör ett viktigt allmänt intresse. När det gäller myndigheters behandling av känsliga personuppgifter måste det enligt regeringen också anses utgöra ett viktigt allmänt intresse att svenska myndigheter, även utanför området för myndighetsutövning, kan bedriva den verksamhet som tydligt faller inom ramen för deras befogenheter på ett korrekt, rättssäkert och effektivt sätt (prop. 2017/18:105 s. 83). Försäkringskassan kan därmed oftast utföra nödvändig behandling av känsliga personuppgifter med stöd av undantaget för ett viktigt allmänt intresse.

Ytterligare en förutsättning för att undantaget i artikel 9.2 g i dataskyddsförordningen ska vara tillämpligt är att behandlingen sker på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet. Att grunden för behandlingen ska vara fastställd i enlighet med unionsrätten eller den nationella rätten innebär inte ett krav på att själva behandlingen av personuppgifter ska vara reglerad. Det är i stället den rättsliga förpliktelsen, arbetsuppgiften av allmänt intresse respektive myndighetsutövningen som ska ha stöd i rättsordningen (prop. 2017/18:105 s. 48 f. och s. 84). Detta krav är uppfyllt ifråga om behandlingar som sker till följd av uppdrag som framgår av Försäkringskassans instruktion, regleringsbrev, specifika regeringsuppdrag, myndighetsförordningen och verksamhetsspecifika lagstiftningar samt när det är nödvändigt för att fatta beslut som påverkar enskilda.

Det rättsliga stödet ska också vara förenligt med det väsentliga innehållet i rätten till dataskydd. Regeringen har uttryckt att det är svårt att föreställa sig en rättslig grund för behandling av personuppgifter som uppfyller kraven i artikel 6 i dataskyddsförordningen, men som ändå inte är förenlig med det väsentliga innehållet i rätten till dataskydd (prop. 2017/18:105 s. 84).

För behandling av känsliga personuppgifter för ett viktigt allmänt intresse krävs också att det finns tillämpliga bestämmelser om skyddsåtgärder. Det kan handla om till exempel bestämmelser om sökbegränsningar, behörighetsbegränsning, loggkontroll, krav på dokumentation, längsta tid för behandling av personuppgifter och gallring. Bestämmelser om sekretess och partsinsyn enligt förvaltningslagen anses också utgöra bestämmelser om skyddsåtgärder.

I dataskyddslagen finns stöd för myndigheters behandling av känsliga personuppgifter i vissa fall. Det är tillåtet för en myndighet att behandla känsliga personuppgifter som lämnats till myndigheten och som därmed är allmänna handlingar. Det är också tillåtet att behandla känsliga personuppgifter om det är nödvändigt för handläggningen av ett ärende. Utanför ren ärendehandläggning får känsliga personuppgifter behandlas om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet. Av förarbetena framgår att tredje punkten inte är avsedd att tillämpas slentrianmässigt i den löpande verksamheten och att det krävs en bedömning av intrånget i den personliga integriteten i varje enskilt fall (prop. 2017/18:105 s. 194).

Kravet på skyddsåtgärder tillgodoses i dataskyddslagen genom ett förbud att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter vid behandling med stöd av första stycket. Sökbegränsningen innebär att det inte är tillåtet att använda känsliga personuppgifter i syfte att exempelvis kartlägga personer på grundval av etnicitet. Däremot kan sökningar göras när syftet med sökningen inte är att identifiera ett urval av individer, till exempel när syftet är att utöva tillsyn, ta fram verksamhetsstatistik eller registervård (prop. 2017/18:105 s. 90 f.).

Dataskyddslagen är subsidiär i förhållande till 114 kap. SFB. Det betyder att bestämmelserna i dataskyddslagen inte ska tillämpas om det finns mer specifika

bestämmelser i en annan lag. Eftersom det finns bestämmelser om behandling av känsliga personuppgifter i 114 kap. SFB, behandlar Försäkringskassan känsliga personuppgifter i kärnverksamheten huvudsakligen med stöd av SFB.

6.6.1 Behandling av känsliga personuppgifter i Försäkringskassans kärnverksamhet

114 kap. 11 § SFB

Sådana personuppgifter som avses i artikel 9.1 i EU:s dataskyddsförordning (känsliga personuppgifter) får behandlas om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggning av ett ärende. Känsliga personuppgifter får också behandlas om det är nödvändigt för något av de ändamål som anges i 9 §.

Känsliga personuppgifter om hälsa får även behandlas om det är

1. nödvändigt för något av de ändamål som anges i 8 § 1 och 2,

2. nödvändigt för något av de ändamål som anges i 8 § 4–7 och uppgifterna behandlas eller har behandlats för något av de ändamål som anges i 8 § 1–3, eller

3. absolut nödvändigt för behandling med stöd av 10 § och uppgifterna behandlas eller har behandlats för något av de ändamål som anges i 8 § 1–3.

I andra fall får känsliga personuppgifter inte behandlas.

Försäkringskassans behandling av känsliga personuppgifter inom ramen för tillämpningsområdet för 114 kap. SFB sker för ett viktigt allmänt intresse med stöd av artikel 9.2 g i dataskyddsförordningen (prop. 2017/18:171 s. 193). Möjligheten att behandla känsliga personuppgifter för ett viktigt allmänt intresse har dock begränsats genom en särskild reglering i 114 kap. 11 § SFB. Begränsningarna utgör en sådan skyddsåtgärd som krävs för att det ska vara tillåtet att behandla känsliga personuppgifter med stöd av artikel 9.2 g i dataskyddsförordningen.

Ingen begränsning för uppgifter som har lämnats i ett ärende eller är nödvändiga för handläggningen av ett ärende

Begränsningen i 114 kap. 11 § SFB omfattar inte all behandling av känsliga personuppgifter. Samtliga kategorier av känsliga personuppgifter får utan begränsning behandlas om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av ett ärende. Känsliga personuppgifter om till exempel hälsa eller sexuell läggning som framgår av en ansökan eller ett läkarintyg får därmed alltid behandlas i ärendehandläggningen. Det är dock viktigt att den som hämtar in kompletterande uppgifter noga överväger om eventuella känsliga personuppgifter är nödvändiga för handläggningen av ärendet.

Ingen begränsning för uppgifter som lämnas ut från myndigheten

Samtliga kategorier av känsliga personuppgifter får också utan begränsning behandlas i syfte att lämnas ut från Försäkringskassan under förutsättning att det sker i överensstämmelse med lag eller förordning, alternativt följer av vissa internationella åtaganden (114 kap. 9 § SFB). Om uppgifter ska lämnas ut med anledning av en reglerad möjlighet eller skyldighet att lämna uppgifter, gäller därmed inga särskilda begränsningar i fråga om känsliga personuppgifter.

Behandling av känsliga personuppgifter om hälsa

Behandling av känsliga personuppgifter om hälsa är knuten till de olika ändamål som anges i 114 kap. 8–10 §§ SFB. Läs mer om ändamålen i avsnitt 5.1.

Vi får behandla känsliga personuppgifter om hälsa om det är nödvändigt för att:

- tillgodose behovet av det underlag som krävs för att den registrerades eller någon annans rättigheter eller skyldigheter i fråga om förmåner och ersättningar ska kunna bedömas eller fastställas (114 kap. 8 § 1 SFB)
- informera om förmåner och ersättningar (114 kap. 8 § 2 SFB).

Känsliga personuppgifter om hälsa som har samlats in i syfte att användas i den handläggande verksamheten eller för de ändamål som anges i 114 kap. 8 § 1 och 2 SFB får därutöver behandlas om det är nödvändigt för att:

- vidta kontrollåtgärder som syftar till att förebygga, förhindra och upptäcka felaktiga utbetalningar och bidragsbrott (114 kap. 8 § 4 SFB)
- planera sina respektive verksamheter (114 kap. 8 § 5 SFB)
- genomföra resultatstyrning, resultatuppföljning, resultatredovisning, utvärdering eller tillsyn (114 kap. 8 § 6 SFB)
- framställa statistik (114 kap. 8 § 7 SFB).

För att känsliga personuppgifter om hälsa ska få användas för att bland annat vidta kontrollåtgärder och utvärdera och följa upp verksamheten, måste uppgifterna alltså ha kommit in till Försäkringskassan genom handläggningen.

Vi får också behandla känsliga personuppgifter om hälsa med stöd av finalitetsprincipen om det är absolut nödvändigt och uppgifterna har samlats in i syfte att användas i den handläggande verksamheten eller för de ändamål som anges i 114 kap. 8 § 1 och 2 SFB. Läs mer om finalitetsprincipen i avsnitt 3.2 och 5.1.9. Kravet på att behandling med stöd av finalitetsprincipen ska vara absolut nödvändig innebär inte att känsliga personuppgifter får behandlas endast i absoluta undantagsfall, utan avser att markera att behandlingen ska ske med restriktivitet och att behovet av att behandla personuppgiften ska prövas noga i det enskilda ärendet (prop. 2023/24:29 s. 100). Utrymmet för vidarebehandling av känsliga personuppgifter begränsas även av artikel 6.4 i dataskyddsförordningen. Av den bestämmelsen följer bland annat att personuppgifternas art, särskilt om det handlar om känsliga personuppgifter, ska beaktas vid en bedömning enligt finalitetsprincipen.

6.6.2 Sökbegränsningar i Försäkringskassans kärnverksamhet

114 kap. 12 § SFB
Sökningar får inte utföras i syfte att få fram ett urval av personer grundat på känsliga personuppgifter.

För de ändamål som anges i 8 § får dock sökningar utföras i syfte att få fram ett urval av personer grundat på känsliga personuppgifter om hälsa, om uppgiften avser förmån eller ersättning eller om urvalet ska användas för att

1. vidta åtgärder i handläggningen,

2. planera, följa upp eller utvärdera handläggningen, eller

3. vidta kontrollåtgärder som syftar till att förebygga, förhindra och upptäcka felaktiga utbetalningar och bidragsbrott.

Försäkringskassan får som huvudregel inte göra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. Det innebär att det inte är tillåtet att sammanställa information utifrån en omständighet som är kategoriserad som känslig personuppgift. Det är till exempel inte tillåtet att göra en sammanställning av personer som har en viss religion eller ett visst etniskt ursprung. Däremot är det tillåtet att göra sökningar på känsliga personuppgifter när syftet inte är att ta fram ett urval av personer, utan det snarare blir en följdeffekt av sökningen. Det kan vara fallet i samband med bland annat registervård. Det är också tillåtet att söka på en enda person.

Från huvudregeln om sökbegränsningar gäller vissa undantag för känsliga personuppgifter om hälsa. Sökningar får utföras för de primära ändamål som anges i 114 kap. 8 § SFB (läs om ändamålen i avsnitt 5.1) i syfte att få fram ett urval av personer grundat på känsliga personuppgifter om hälsa om någon av följande förutsättningar är uppfylld:

- Uppgiften avser en förmån eller ersättning.
- Urvalet ska användas för att vidta åtgärder i handläggningen.
- Urvalet ska användas för att planera, följa upp eller utvärdera handläggningen.
- Urvalet ska användas för att vidta kontrollåtgärder som syftar till att förebygga, förhindra och upptäcka felaktiga utbetalningar och bidragsbrott.

Det är alltså tillåtet att söka efter och sortera ärenden baserat på uppgifter om de förmåner eller ersättningar ärendena gäller. Det är exempelvis möjligt att söka fram uppgifter om personer som beviljats en sjukförsäkringsförmån under en viss period.

Det är också tillåtet att använda mer specifika uppgifter om hälsa som urvalskriterium för att bland annat fördela ärenden, följa upp och utvärdera handläggningen. Sådana mer specifika uppgifter kan vara diagnoser eller funktionsnedsättningar.

I olika modeller för analys och urval som används i syfte att förebygga, förhindra och upptäcka felaktiga utbetalningar och bidragsbrott är det möjligt att använda uppgifter om hälsa i syfte att identifiera de ärenden som behöver kontrolleras.

Undantaget från huvudregeln om sökbegränsningar gäller inte vid behandling av personuppgifter för utlämnanden enligt 114 kap. 9 § SFB.

6.7 Behandling för arkiv-, forsknings- och statistikändamål

Artikel 9.2 j i dataskyddsförordningen

Punkt 1 ska inte tillämpas om något av följande gäller:

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.

Undantaget i artikel 9.2 j i dataskyddsförordningen avser nödvändig behandling av känsliga personuppgifter för bland annat arkivändamål av allmänt intresse och statistiska ändamål. Behandlingen ska ske på grundval av unionsrätten eller medlemsstaternas nationella rätt, som ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om skyddsåtgärder. Läs mer om vad detta innebär i avsnitt 6.6.

6.7.1 Arkivändamål

3 kap. 6 § första stycket dataskyddslagen

Känsliga personuppgifter får behandlas för arkivändamål av allmänt intresse med stöd av artikel 9.2 j i EU:s dataskyddsförordning, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om arkiv.

Bestämmelsen förtydligar att dataskyddsförordningen och dataskyddslagen inte hindrar att myndigheter arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. Regeringen har ansett att det skydd som enligt svensk rätt gäller för myndigheters arkiv uppfyller kraven på lämpliga och särskilda åtgärder (prop. 2017/18:105 s. 116).

Försäkringskassan utför nödvändig behandling av känsliga personuppgifter för arkivändamål av allmänt intresse med stöd av arkivlagen, arkivförordningen och Riksarkivets föreskrifter, bland annat de föreskrifter som har meddelats med stöd av 7 § förordningen om behandling av personuppgifter vid Försäkringskassan och Pensionsmyndigheten.

Personuppgifter som behandlas enbart för arkivändamål av allmänt intresse får enligt 4 kap. 1 § dataskyddslagen användas för att vidta åtgärder i fråga om den registrerade endast om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen. Med vitala intressen avses intressen som är av avgörande betydelse för den registrerades liv. Bestämmelsen skulle t.ex. kunna aktualiseras om arkiverade uppgifter måste användas för att identifiera och kontakta personer som utan deras vetskap har exponerats för farliga ämnen (prop. 2017/18:105 s 200).

6.7.2 Statistikändamål

3 kap. 7 § dataskyddslagen
Känsliga personuppgifter får behandlas med stöd av artikel 9.2 j i EU:s dataskyddsförordning, om behandlingen är nödvändig för statistiska ändamål och samhällsintresset av det statistikprojekt där behandlingen ingår klart väger över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan innebära.

15 § lagen om den officiella statistiken
Personuppgifter som avses i artikel 9.1 (känsliga personuppgifter) och artikel 10 i EU:s dataskyddsförordning får behandlas om det följer av föreskrifter som regeringen meddelar.

Vid framställning av annan statistik än officiell statistik får personuppgifter enligt första stycket också behandlas om behandlingen

1. är nödvändig för statistiska ändamål och samhällsintresset av det statistikprojekt där behandlingen ingår klart väger över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan innebära, eller

2. ingår i ett forskningsprojekt och behandlingen har godkänts enligt lagen (2003:460) om etikprövning av forskning som avser människor.

8 § förordningen om den officiella statistiken
I bilagan anges när det är tillåtet att behandla sådana personuppgifter som avses i 15 § lagen om den officiella statistiken.

Med statistiska ändamål avses enligt dataskyddsförordningen varje åtgärd som vidtas för den insamling och behandling av personuppgifter som är nödvändig för statistiska undersökningar eller för framställning av statistiska resultat. 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 fysisk person. (Skäl 162 till dataskyddsförordningen)

En bestämmelse om intresseavvägning i 3 kap. 7 § dataskyddslagen tillgodoser behovet av skyddsåtgärd vid nödvändig behandling av känsliga personuppgifter för statistiska ändamål. Intresseavvägningen ska ske genom en helhetsbedömning av samtliga omständigheter. Vid bedömningen bör beaktas bland annat statistikprojektets samhällsintresse och behovet av personuppgifter i projektet. Den personuppgiftsansvariga måste också noga överväga möjligheten att i stället inhämta de registrerades samtycke. Vid bedömningen av intrånget i den enskildes personliga integritet ska vikt läggas vid sådana aspekter som uppgifternas känslighet, den inställning de registrerade kan antas ha till behandlingen, säkerheten vid behandlingen och risken för att uppgifterna sprids eller att enskilda personer skulle kunna identifieras i statistiken. (Prop. 2017/18:105 s. 197 f.)

Personuppgifter som behandlas enbart för statistiska ändamål får enligt 4 kap. 2 § dataskyddslagen användas för att vidta åtgärder i fråga om den registrerade endast om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen.

Ytterligare begränsningar av när det är tillåtet att behandla känsliga personuppgifter för statistiska ändamål regleras i lagen och förordningen om den officiella statistiken.

Försäkringskassan ansvarar för officiell statistik som gäller stöd till familjer och barn respektive stöd vid sjukdom och funktionsnedsättning. Av bilagan till förordningen om den officiella statistiken följer att vi endast får behandla känsliga personuppgifter som avser enskilda personers hälsotillstånd för framställning av sådan officiell statistik som vi ansvarar för.

Vid framställning av så kallad annan statistik än officiell statistik finns ingen begränsning av vilka kategorier av känsliga personuppgifter som får behandlas. Behandlingen ska dock vara nödvändig för statistiska ändamål och samhällsintresset av statistikprojektet ska klart överstiga den risk för otillbörligt intrång i den enskildes personliga integritet som behandlingen kan innebära. Känsliga personuppgifter får också behandlas om behandlingen ingår i ett forskningsprojekt och har godkänts enligt lagen (2003:460) om etikprövning av forskning som avser människor.

Försäkringskassan kan även behandla känsliga personuppgifter för statistikändamål med stöd av 114 kap. SFB. Läs mer om det i avsnitt 5.1.6 och 6.6.1.

6.8 Behandling enligt visselblåsarlagen

Det finns inte några särskilda bestämmelser om behandling av känsliga personuppgifter i visselblåsarlagen. Om känsliga personuppgifter förekommer i ett uppföljningsärende ska vi därför tillämpa dataskyddsförordningen och dataskyddslagen.

6.9 Särskilt skyddsvärda personuppgifter

Vissa kategorier av personuppgifter anses särskilt skyddsvärda utan att vara känsliga personuppgifter i dataskyddsförordningens mening. Uppgifter av sådan särskilt skyddsvärd karaktär är framför allt personuppgifter om lagöverträdelser och personnummer respektive samordningsnummer. Det finns dock även andra kategorier av uppgifter som av olika skäl bör skyddas särskilt.

6.9.1 Personuppgifter om lagöverträdelser

Artikel 10 i dataskyddsförordningen
Behandling av personuppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott 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.

3 kap. 8 § första stycket dataskyddslagen
Personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning får behandlas av myndigheter.

Personuppgifter om lagöverträdelser är enligt IMY:s rättsliga ställningstagande IMYRS 2021:1 uppgifter om att någon har

- begått ett brott
- blivit fälld eller friad i domstol i ett brottmål
- blivit föremål för så kallade straffprocessuella tvångsmedel, till exempel häktning, reseförbud eller beslag
- misstänkts för ett konkret brott.

Av artikel 10 i dataskyddsförordningen och 3 kap. 8 § dataskyddslagen följer att det inte finns några särskilda begränsningar för myndigheter att behandla personuppgifter om lagöverträdelser. I likhet med vad som gäller all övrig personuppgiftsbehandling krävs att det finns en tillämplig rättslig grund (avsnitt 4). Övriga bestämmelser i dataskydds-förordningen och eventuellt tillämplig registerförfattning ska också vara uppfyllda.

Enligt EU-domstolens praxis finns det tre kriterier som är relevanta vid bedömningen av om en lagöverträdelse avser brott:

1. Den rättsliga kvalificeringen av överträdelsen i nationell rätt.
2. Överträdelsens art.
3. Strängheten i den sanktion som den berörde kan åläggas.

Överträdelser kan anses ha en straffrättslig karaktär även om de inte kvalificeras som straffrättsliga i nationell rätt. (EU-domstolens dom Latvijas Republikas Saeima, C-439/19, EU:C:2021:504, punkt 87)

Uttrycket sammanhängande säkerhetsåtgärder har bedömts vara likvärdigt med straffprocessuella tvångsmedel (prop. 2017/18:105 s. 198).

Försäkringskassan ansvarar för officiell statistik som gäller stöd till familjer och barn respektive stöd vid sjukdom och funktionsnedsättning. Vid framställning av sådan statistik saknas stöd för att behandla personuppgifter om lagöverträdelser (15 § första stycket lagen om den officiella statistiken).

Enligt IMY utgör en uppgift om att någon har eller kan ha begått något visst brott en personuppgift som rör en lagöverträdelse som innefattar brott, även om det inte finns något rättsligt förfarande om ett eventuellt brott (IMY:s rättsliga ställningstagande IMYRS 2021:1). Ett rättsligt förfarande kan exempelvis vara en förundersökning eller en domstolsprocess.

Vid framställning av så kallad annan statistik än officiell statistik får Försäkringskassan behandla personuppgifter om lagöverträdelser om behandlingen är nödvändig för statistiska ändamål och samhällsintresset av statistikprojektet klart överstiger den risk för otillbörligt intrång i den enskildes personliga integritet som behandlingen kan innebära. Personuppgifter om lagöverträdelser får också behandlas om behandlingen ingår i ett forskningsprojekt och har godkänts enligt lagen (2003:460) om etikprövning av forskning som avser människor. (15 § andra stycket lagen om den officiella statistiken)

6.9.2 Personnummer och samordningsnummer

3 kap. 10 § dataskyddslagen

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

I 3 kap. 10 § dataskyddslagen finns en bestämmelse om personnummer och samordningsnummer som har sin grund i artikel 87 i dataskyddsförordningen, som tillåter särskilda villkor för behandlingen av nationella identifikationsnummer. Den innebär att det ska göras en intresseavvägning mellan behovet av behandlingen och de integritetsrisker som den innebär. I bedömningen bör man bland annat ta hänsyn till behandlingens omfattning och om det är möjligt att uppnå syftet med behandlingen på ett annat sätt (prop. 2017/18:105 s. 199).

Personnummer och samordningsnummer får alltid behandlas med samtycke. Myndigheter bör dock inte använda samtycke som rättslig grund för behandling av personuppgifter (skäl 43 till dataskyddsförordningen).

I Försäkringskassans kärnverksamhet är det viktigt med säker identifikation. Det är därför i de flesta fall motiverat att behandla personnummer och samordningsnummer.

6.9.3 Andra särskilt skyddsvärda personuppgifter

Skyddade personuppgifter är det samlingsnamn som Skatteverket använder för de olika skyddsåtgärderna skyddad folkbokföring, sekretessmarkering och fingerade personuppgifter. Dessa skyddsåtgärder används för personer som behöver ett utökat skydd för uppgifter om den egna personen, exempelvis någon som lever under hot eller trakasserier eller är förföljd. Skatteverket beslutar om skyddad folkbokföring och sekretessmarkering medan Polismyndigheten beslutar om fingerade personuppgifter. Skyddade personuppgifter omnämns inte i dataskyddsförordningen, men får anses vara särskilt skyddsvärda.

Läs mer
Läs mer om hur skyddade personuppgifter ska hanteras på Försäkringskassan i Försäkringskassans vägledning (2001:3) *Offentlighet, sekretess och utlämnande av handlingar och uppgifter* och Försäkringskassans riktlinjer (2011:34) *Hantering av skyddade personuppgifter inom Försäkringskassan.*

IMY anser att även löneuppgifter och värderande uppgifter, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler, kan vara särskilt skyddsvärda (IMY:s webbplats).

7 Dataskydd när personuppgifter lämnas ut från Försäkringskassan

Personuppgifter lämnas ut från Försäkringskassan av olika skäl. Det kan handla om att någon begär eller frågar efter uppgifter, att vi bedömer att en annan myndighet har behov av vissa uppgifter, att det finns en skyldighet att underrätta en aktör om vissa uppgifter eller att vi behöver lämna ut uppgifter, till exempel personnummer, i syfte att kunna inhämta uppgifter.

7.1 Ett utlämnande av personuppgifter är en personuppgiftsbehandling

Ett utlämnande av personuppgifter medför nästan alltid en behandling i dataskyddslagstiftningens mening, oavsett om själva utlämnandet sker manuellt eller inte. Det beror på att uppgifterna i de flesta fall måste hämtas från ett it-system. Det krävs därför stöd i en rättslig grund enligt artikel 6 i dataskyddsförordningen för att personuppgifter ska få lämnas ut.

Oftast lämnar Försäkringskassan ut personuppgifter för att fullgöra en rättslig förpliktelse (artikel 6.1 c i dataskyddsförordningen), som ett led i myndighetsutövning eller för att utföra en uppgift av allmänt intresse (artikel 6.1 e i dataskyddsförordningen). Den rättsliga grunden ska i sådana fall vara fastställd, vilket innebär att den rättsliga förpliktelsen, uppgiften av allmänt intresse respektive myndighetsutövningen ska ha stöd i rättsordningen. Den rättsliga grunden ska med andra ord vara rättsligt förankrad. Läs mer om rättslig grund i kapitel 4.

Det är olämpligt att använda samtycke som rättslig grund vid utlämnande av personuppgifter som avser registrerade som befinner sig i underläge till Försäkringskassan (jfr avsnitt 4.2.1). Det gäller även om samtycke tillämpas som grund för att bryta eventuell sekretess (se vägledningen [2001:3] Offentlighet, sekretess och utlämnande av handlingar och uppgifter).

Ett utlämnande ska också uppfylla de grundläggande kraven i artikel 5 i dataskydds-förordningen (se kapitel 3).

Rättslig förankring av den rättsliga grunden

För att den rättsliga grunden ska anses förankrad krävs att det finns bestämmelser som medför ett behov av att behandla personuppgifter. Den rättsliga grunden kan vara förankrad i exempelvis Försäkringskassans instruktion, regleringsbrev, specifika regeringsuppdrag, myndighetsförordningen, reglerade uppgiftsskyldigheter eller skyldigheten för myndigheter att på begäran lämna uppgiften till varandra enligt 6 kap. 5 § OSL. Bestämmelser om sekretess eller sekretessgenombrott ger i sig inte stöd för att behandla personuppgifter.

Vid kommunicering i ett ärende finns exempelvis förankringen av den rättsliga grunden för personuppgiftsbehandlingen i 25 § FL, som reglerar ett krav på kommunikation. Vid partsinsyn finns förankringen i 10 § FL, som fastställer partens rätt att ta del av upp-gifter. Stödet för behandlingen av personuppgifter finns alltså inte i 10 kap. 3 § OSL, som bryter eventuell sekretess.

När Försäkringskassan lämnar ut personuppgifter i ett ärende i syfte att kunna efterfråga eller begära uppgifter inom ramen för handläggningen, är den rättsliga grunden oftast förankrad i verksamhetsspecifika lagstiftningar, till exempel 110 kap. 14 § och 31–34 a §§ SFB eller 4 kap. 9 § lagen (2008:145) om statligt tandvårdsstöd.

Vid en myndighets begäran om uppgifter kan den rättsliga grunden vara förankrad i 6 kap. 5 § OSL. Vid utlämnande med stöd av en uppgiftsskyldighet är den rättsliga grunden dock ofta förankrad i själva uppgiftsskyldigheten, som både bryter sekretess och ger stöd för personuppgiftsbehandlingen. Sådana uppgiftsskyldigheter finns till exempel i LUFFA. Även den generella sekretessbrytande bestämmelsen i 10 kap. 15 a § OSL både bryter sekretess och ger stöd för personuppgiftsbehandlingen (prop. 2024/25:180 s. 80).

Ändamål vid utlämnande

När personuppgifter lämnas ut, måste det fastställas ett ändamål för behandlingen. Oftast är det relativt enkelt att fastställa ändamålet. Om behandlingen sker till följd av en skyldighet eller ett åtagande att lämna uppgifter, är ändamålet att fullgöra den aktuella skyldigheten eller åtagandet. Det kan handla om att till exempel fullgöra en uppgifts-skyldighet, fullgöra en skyldighet att lämna ut allmänna handlingar eller att lämna uppgifter i enlighet med ett avtal om informationsutbyte.

Om personuppgifter lämnas ut på Försäkringskassans eget initiativ med stöd av 10 kap. 15 a § OSL, kan ändamålet fastställas med stöd av de syften som anges i paragrafen.

Efter att personuppgifter har samlats in för ett visst ändamål, får de som huvudregel inte behandlas för ett ändamål som är oförenligt med det ursprungliga ändamålet (läs mer om finalitetsprincipen i avsnitt 3.2). Uppgifter får dock behandlas i strid med det ursprungliga ändamålet om det sker i enlighet med en uppgiftsskyldighet (jämför prop. 2023/24:29 s. 47 f.). Försäkringskassan behöver inte heller ta ställning till om ett utlämnande av personuppgifter enligt 6 kap. 5 § eller 10 kap. 15 § OSL är förenligt med de ändamål som personuppgifterna har samlats in för (HFD 2021 ref. 10 respektive prop. 2024/25:180 s. 80).

Sammanställningar eller sökningar vid utlämnande

Ibland behöver personuppgifter sammanställas eller sökas fram innan de kan lämnas ut. Även det innebär behandling av personuppgifter. Sådan behandling sker för samma rättsliga grund och ändamål som själva utlämnandet.

Enligt 114 kap. 12 § SFB gäller vissa begränsningar när vi gör sökningar som omfattar känsliga personuppgifter. Sökbegränsningarna aktualiserar begränsningsregeln i 2 kap. 7 § TF, vilket innebär att en sammanställning som innehåller personuppgifter bör ses som en allmän handling endast om vi med beaktande av sökbegränsningen får ta fram den för ett internt syfte i vår egen verksamhet (prop. 2023/24:29 s. 69). Sökbegränsningarna gäller även vid en begäran enligt 6 kap. 5 § OSL.

Undantagen i 114 kap. 12 § andra stycket SFB ska tillämpas vid en begäran om en allmän handling enligt TF, men gäller inte vid en begäran om uppgifter enligt 6 kap. 5 § OSL (KRNS mål nr 2452-25).

Läs mer

Läs mer om hur sökbegränsningarna påverkar möjligheten att göra sammanställningar vid utlämnanden i Försäkringskassans vägledning (2001:3) *Offentlighet, sekretess och utlämnande av handlingar och uppgifter*.

7.2 Utlämnande av personuppgifter i Försäkringskassans kärnverksamhet

114 kap. 8 § punkt 3 och 4 SFB
Försäkringskassan och Pensionsmyndigheten får behandla personuppgifter om det är nödvändigt för att

3. handlägga ärenden,

4. vidta kontrollåtgärder som syftar till att förebygga, förhindra och upptäcka felaktiga utbetalningar och bidragsbrott,

114 kap. 9 § SFB
Personuppgifter som behandlas för ändamål som anges i 8 § får behandlas av Försäkringskassan och Pensionsmyndigheten även för att fullgöra uppgiftslämnande som

1. sker i överensstämmelse med lag eller förordning, eller

2. följer av unionsrätten, åtaganden i samarbetet inom Europeiska ekonomiska samarbetsområdet eller avtal om social trygghet eller utgivande av sjukvårdsförmåner som Sverige ingått med andra stater.

Försäkringskassan får enligt 114 kap. 9 § SFB lämna ut personuppgifter som behandlas i vår kärnverksamhet under förutsättning att det sker i överensstämmelse med lag eller förordning. I vissa fall kan vi också lämna ut personuppgifter för de ändamål som anges i 114 kap. 8 § SFB. När uppgifter efterfrågas med stöd av exempelvis 110 kap. 14 § SFB kan det vara nödvändigt att lämna ut personnummer för att identifiera den person som de efterfrågade uppgifterna gäller. Då lämnas personuppgifter ut med stöd av de ändamålen som avser handläggning eller kontrollåtgärder. Visst utlämnande kan även ske med stöd av den så kallade finalitetsprincipen.

Ändamålsbestämmelserna i 114 kap. SFB innebär inget självständigt stöd för utlämnande av personuppgifter. Trots att det finns ett angivet ändamål i 114 kap. SFB, ska vi identifiera den rättsliga grunden och den rättsliga förankringen.

I likhet med vad som gäller övriga utlämnanden ska vi alltid beakta de grundläggande kraven i artikel 5 i dataskyddsförordningen.

Digitalt utlämnande av uppgifter inom Försäkringskassans förmånsverksamhet

114 kap. 14 § SFB
Direktåtkomst till personuppgifter i sådan verksamhet som avses i 2 § är tillåten endast i den utsträckning som anges i lag eller förordning.

4 § förordningen om behandling av personuppgifter vid Försäkringskassan och Pensionsmyndigheten
Pensionsmyndigheten får ha direktåtkomst till personuppgifter hos Försäkringskassan om beviljad och utbetald sjukersättning, aktivitetsersättning och livränta samt arbetsskada, för att

1. fastställa pensionsrätt för allmän ålderspension,

2. bedöma om allmän ålderspension kan lämnas utan föregående ansökan, eller

3. bedöma och beräkna rätten till allmän ålderspension, efterlevandepension eller efterlevandestöd.

Vid direktåtkomst enligt första stycket har Pensionsmyndigheten rätt att ta del av de personuppgifter som omfattas av åtkomsten.

5 § förordningen om behandling av personuppgifter vid Försäkringskassan och Pensionsmyndigheten
Arbetsförmedlingen och sådana kommuner och regioner som deltar i samverkan och finansiell samordning inom rehabiliteringsområdet får ha direktåtkomst till personuppgifter hos Försäkringskassan i den utsträckning den registrerade samtycker till det. Endast de personer vid nämnda myndigheter som ansvarar för den lokala samverkansaktivitet i vilken den registrerade deltar får ges behörighet för direktåtkomst till sådana personuppgifter.

6 § förordningen om behandling av personuppgifter vid Försäkringskassan och Pensionsmyndigheten
Den registrerade får ha direktåtkomst till sådana personuppgifter om sig själv hos Försäkringskassan och Pensionsmyndigheten som får lämnas ut till honom eller henne. Vid sådan direktåtkomst ska den registrerades identitet kontrolleras genom en säker metod för identifiering.

Försäkringskassan kan lämna ut uppgifter i kärnverksamheten digitalt på två sätt:

- Genom direktåtkomst, som innebär att mottagaren har elektronisk tillgång till uppgifterna hos Försäkringskassan.
- Genom annat elektroniskt utlämnande än direktåtkomst, till exempel via mejl, fil, fråga/svar-tjänster eller internet.

För att Försäkringskassan ska kunna lämna uppgifter genom direktåtkomst krävs särskild reglering. Uppgifter kan lämnas ut elektroniskt på annat sätt än genom direktåtkomst under förutsättning att det finns stöd för att lämna uppgifterna och uppgiftslämnandet sker på ett tillräckligt säkert sätt.

Innebörden av uttrycket direktåtkomst är att någon utomstående har direkt tillgång till uppgifter som behandlas hos Försäkringskassan. Den utomstående kan på egen hand ta fram uppgifter och på så sätt få uppgifter utlämnade till sig. Prövningen av om ett

utlämnande är förenligt med OSL måste därför göras redan då uppgifterna görs tillgängliga för direktåtkomst, oavsett om någon mottagare vid den tidpunkten tar del av dem eller inte. Den faktiska begränsningen av direktåtkomsten görs sedan med hjälp av olika tekniska lösningar beroende på hur omfattningen av direktåtkomsten har begränsats i det enskilda fallet.

En rättslig konsekvens av direktåtkomst är att de uppgifter eller handlingar hos den utlämnande myndigheten som direktåtkomsten omfattar blir expedierade i den mening som avses i 2 kap. 10 § TF redan i och med att systemet för direktåtkomst tas i bruk. Direktåtkomst medför därmed att handlingarna är att anse som allmänna både hos den utlämnande och mottagande myndigheten. Det har ingen betydelse om den mottagande myndigheten faktiskt har använt sig av direktåtkomsten (jämför prop. 2007/08:160 s. 164 och HFD 2011 ref. 52).

Ibland kan det vara svårt att avgöra om uppgifter lämnas ut med direktåtkomst eller genom annat elektroniskt utlämnande. HFD har gjort förtydliganden av vad som ska betraktas som direktåtkomst i det så kallade LEFI-Online-målet.

Rättsfall

Frågan i målet var om ett utlämnande via Försäkringskassans fråga/svarstjänst LEFI Online var att anse som direktåtkomst. HFD bedömde att det var avgörande om den aktuella upptagningen kan anses förvarad hos den mottagande myndigheten enligt (nuvarande 2 kap. 6 § första stycket) TF, det vill säga om den är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas. Försäkringskassan ansågs förfoga över frågan om, och i så fall vilka, uppgifter som skulle lämnas ut, eftersom ett utlämnande genom LEFI Online förutsätter att Försäkringskassan reagerar på en begäran om att de efterfrågade uppgifterna ska lämnas ut. Någon sådan teknisk tillgång till upptagningar som avses i 2 kap. 6 § första stycket TF bedömdes därmed inte föreligga. Detta innebar att förfarandet inte var att betrakta som direktåtkomst. (HFD 2015 ref. 61)

LEFI Online-målet rörde enbart begreppet direktåtkomst enligt SFB, men HFD har senare konstaterat att en myndighet har direktåtkomst till uppgifter hos en annan myndighet om uppgifterna finns i en upptagning som i tryckfrihetsförordningens mening kan anses förvarad hos den förstnämnda myndigheten (HFD 2020 not 16). LEFI-domen har därmed givits generell tillämplighet.

Direktåtkomst till personuppgifter i förmånsverksamheten är endast tillåtet i den utsträckning som anges i lag eller förordning. I förordningen om behandling av personuppgifter vid Försäkringskassan och Pensionsmyndigheten finns vissa bestämmelser som tillåter direktåtkomst.

7.3 Särskilt om utlämnande vid begäran om allmän handling

1 kap. 7 § dataskyddslagen

EU:s dataskyddsförordning och denna lag ska inte tillämpas i den utsträckning det skulle strida mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Det finns ingen skyldighet enligt 2 kap. TF att lämna ut en allmän handling digitalt i andra fall än när en sådan skyldighet följer av en annan lag (jämför 2 kap. 16 § TF).

Även om uppgifter lämnas manuellt, innebär ett utlämnande av personuppgifter oftast en behandling enligt dataskyddsförordningen (se avsnitt 1.2.3). Dataskydds-bestämmelserna påverkar som utgångspunkt dock inte Försäkringskassans skyldighet att på begäran lämna ut en allmän handling enligt 2 kap. TF, eftersom dataskyddsförordningen och dataskyddslagen inte ska tillämpas i den utsträckning det skulle strida mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Sekretess på grund av behandling i strid med dataskyddsreglering

Det kan ändå vara aktuellt att beakta dataskyddsbestämmelserna vid en begäran om allmän handling, eftersom sekretess gäller för en personuppgift om det kan antas att uppgiften efter ett utlämnande kommer att behandlas i strid med dataskydds-förordningen eller dataskyddslagen (21 kap. 7 § OSL). Enligt HD hindrar bestämmelsen i 1 kap. 7 § dataskyddslagen inte att dataskyddsförordningens krav beaktas vid tillämpningen av den särskilda sekretessbestämmelsen i 21 kap. 7 § OSL.

Rättsfall

Den myndighet som ska göra en prövning enligt 21 kap. 7 § OSL ska bedöma om uppgifterna efter ett utlämnande kan antas komma att behandlas i strid med bestämmelserna i dataskyddsförordningen, utan att ta ställning till i vilken mån den svenska regleringen innebär att dataskyddsförordningen inte ska tillämpas i den verksamhet som bedrivs av den som har begärt att få ut uppgifterna. Dataskyddsförordningen kan vid tillämpningen av 21 kap. 7 § OSL då närmast ses som en fristående måttstock för när sekretess råder för uppgifter som annars skulle ha varit offentliga. (NJA 2025 s. 123 [I och II])

En bedömning enligt 21 kap. 7 § OSL behöver göras endast om det finns konkreta omständigheter som indikerar att mottagaren kommer att behandla uppgifterna på ett sätt som strider mot dataskyddsregleringen, till exempel att det är fråga om ett massuttag eller selekterat uttag. Någon fullständig bedömning av om behandlingen kommer att strida mot dataskyddsförordningen eller dataskyddslagen behöver inte göras (jämför prop. 2017/18:105 s. 135 f.).

Förbehåll enligt 10 kap. 14 § OSL kan i vissa fall vara ett sätt att balansera integritetsintresset i förhållande till intresset av att lämna ut allmänna handlingar (HFD mål nr Ä9385-25).

Läs mer

Läs mer om bestämmelsen i 21 kap. 7 § OSL i Försäkringskassans vägledning (2001:3) *Offentlighet, sekretess och utlämnande av handlingar och uppgifter*.

Utlämnande av stora mängder personuppgifter

EU-domstolen har uttalat att även om allmänhetens tillgång till allmänna handlingar utgör ett allmänt intresse som kan motivera att personuppgifter som förekommer i sådana handlingar lämnas ut, måste det säkerställas att allmänhetens tillgång till allmänna handlingar är förenlig med de grundläggande rättigheterna som gäller respekt för privatlivet och skydd för personuppgifter. Undantag från dessa rättigheter måste föregås av en proportionalitetsbedömning (se bland annat EU-domstolens dom Latvijas Republikas Saeima, C-439/19, EU:C:2021:504, punkt 120). Om en begäran om allmän handling avser stora mängder personuppgifter, kan det mot bakgrund av detta finnas anledning för Försäkringskassan att göra ytterligare överväganden.

7.4 Säkerhetskrav gäller vid all behandling av personuppgifter

Ett utlämnande av personuppgifter måste alltid ske i enlighet med bestämmelserna om krav på tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå (artikel 32 i dataskyddsförordningen). Det gäller oavsett om utlämnandet sker inom ramen för 114 kap. SFB eller med stöd av dataskyddsförordningen och dataskyddslagen. Det kan påverka på vilket sätt uppgifterna kan lämnas. Det finns ingen skyldighet att lämna uppgifter på det sätt som mottagaren vill.

När vi lämnar ut personuppgifter digitalt, till exempel i ett mejl, måste vi ta hänsyn till Försäkringskassans anvisningar (2022:09) *Säkerhet på Försäkringskassan*.

Läs mer

Läs mer om att lämna ut handlingar eller uppgifter i Försäkringskassans vägledning (2001:3) *Offentlighet, sekretess och utlämnande av handlingar och uppgifter* och Försäkringskassans riktlinjer (2011:7) *Utlämnande av allmänna handlingar och uppgifter*.

8 Tredjelandsöverföring

Om en personuppgiftsbehandling innebär att personuppgifter överförs till ett land utanför EU/EES, ett så kallat tredjeland, gäller särskilda bestämmelser i kapitel V i dataskydds-förordningen.

EDPB har fastställt tre kriterier, som samtliga ska vara uppfyllda, för att en behandling ska anses vara en *tredjelandsöverföring* (se EDPB:s riktlinjer 05/2021 om samspelet mellan tillämpningen av artikel 3 och bestämmelserna om internationella överföringar enligt kapitel V i dataskyddsförordningen):

- En personuppgiftsansvarig eller ett personuppgiftsbiträde omfattas av dataskyddsförordningen för den aktuella behandlingen.
- Den personuppgiftsansvariga eller personuppgiftsbiträdet gör personuppgifterna tillgängliga för en annan personuppgiftsansvarig eller ett personuppgiftsbiträde.
- Den som uppgifterna görs tillgängliga för, som inte behöver omfattas av dataskyddsförordningen, finns i tredjeland.

Det kan vara fråga om en tredjelandsöverföring om Försäkringskassan till exempel anlitar ett personuppgiftsbiträde i ett land utanför EU/EES eller om vi skickar personuppgifter till en mottagare i ett land utanför EU/EES. Att ge någon utanför EU/EES tillgång, exempelvis läsbehörighet, till personuppgifter som finns lagrade inom EU/EES kan också vara en tredjelandsöverföring.

Rättsfall
EU-domstolen har i det så kallade Bodil-målet bedömt att det inte är fråga om någon överföring av uppgifter till tredje land i den mening som avses i direktiv 95/46 vid publicering av uppgifter på internet, när servern tillhandahålls av en leverantör som är etablerad i ett medlemsland och uppgifterna blir allmänt åtkomliga, inklusive från tredjeland (EU-domstolens dom Lindqvist, C-101/01, EU:C:2003:596).

HD hänvisade till EU-domstolens bedömning i Bodil-målet och ogillade ett åtal för brott mot överföringsförbudet i personuppgiftslagen när en rektor hade publicerat personuppgifter på skolans webbplats. Det framgår inte av rättsfallet var servern med skolans webbplats fanns eller vem som innehade servern. (NJA 2005 s. 361)

Bestämmelserna om tredjelandsöverföring gäller även vid överföring till internationella organisationer.

8.1 När är en tredjelandsöverföring tillåten?

För en tredjelandsöverföring av personuppgifter gäller samma krav som för övrig behandling av personuppgifter. Det innebär bland annat att det ska finnas en tillämplig rättslig grund enligt artikel 6 och att de grundläggande principerna enligt artikel 5 ska vara uppfyllda.

För att en tredjelandsöverföring ska vara tillåten krävs dessutom att det finns stöd för överföringen i artiklarna 45–49 i dataskyddsförordningen. En tredjelandsöverföring kan till exempel vara tillåten om EU-kommissionen har fattat beslut om att det aktuella landet har en tillräckligt hög skyddsnivå (adekvat skyddsnivå) eller om utlämnande och mottagande part förbinder sig att tillämpa EU-kommissionens standardavtalsklausuler,

vissa uppförandekoder eller certifieringar. För Försäkringskassan utgör vissa avtal och konventioner mellan stater grund för överföring av uppgifter till tredjeland.

Läs mer
Avtal och konventioner mellan Sverige och andra stater beskrivs i Försäkringskassans vägledning (2017:01) Övergripande bestämmelser i SFB, unionsrätten och internationella avtal.

8.1.1 Beslut om adekvat skyddsnivå

Artikel 45.1 i dataskyddsförordningen
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.

EU-kommissionen har beslutat att skyddsnivån är adekvat i bland annat Storbritannien, Schweiz, Färöarna, Andorra, Sydkorea och Nya Zeeland.

Kanada har bedömts ha en adekvat skyddsnivå under förutsättning att landets lagstiftning för skydd av personuppgifter i privat sektor är tillämplig på mottagarens personuppgiftsbehandling.

EU-kommissionen har även beslutat att skyddsnivån i USA är adekvat under förutsättning att mottagaren omfattas av ”EU–U.S. Data Privacy Framework”. Adekvansbeslutet gäller fortfarande i november 2026 trots att Privacy and Civil Liberties Oversight Board (PCLOB), vars funktion utgör en viktig komponent i skyddet för personuppgifter, inte har varit beslutsför sedan januari 2025.

På IMY:s webbplats finns aktuell information om vilka länder som har en adekvat skyddsnivå.

8.1.2 Lämpliga skyddsåtgärder

Artikel 46.1 i dataskyddsförordningen
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.

De lämpliga skyddsåtgärder som avses i artikel 46 är bland annat standardavtals-klausuler, bindande företagsbestämmelser, uppförandekoder, certifieringar och internationella avtal.

EU-kommissionen beslutade den 4 juni 2021 om standardavtalsklausuler som kan införas i avtal med mottagare i tredjeland. Klausulerna innehåller skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden som

- vill föra över personuppgifter till länder utanför EU/EES
- som tar emot sådana uppgifter.

Klausulerna reglerar också andra frågor kring överföringen, till exempel de registrerades rättigheter och hur tvister med anledning av avtalet ska lösas.

Bindande företagsbestämmelser kan användas inom multinationella företag och är inte aktuella för myndigheter.

En uppförandekod är en uppsättning dataskyddsregler för vissa kategorier av personuppgiftsansvariga eller personuppgiftsbiträden, som de frivilligt tar på sig att följa. I Sverige är det IMY som godkänner uppförandekoder. Redan godkända uppförandekoder finns samlade i register hos EDPB.

Certifieringsordningar innehåller kriterier som personuppgiftsansvariga och personuppgiftsbiträden kan tillämpa för att visa att de lever upp till dataskydds-förordningens skyldigheter och principen om ansvarsskyldighet. Kriterierna i en certifieringsordning kan exempelvis handla om vilka tekniska och organisatoriska skyddsåtgärder som en personuppgiftsansvarig ska införa. Certifieringsordningen granskas av IMY och EDPB. Därefter är Swedac ackrediteringsorgan.

Det finns ett flertal internationella avtal om social trygghet som medför skyldigheter för Försäkringskassan att lämna personuppgifter till tredjeland.

Läs mer
På intranätet Fia kan du läsa mer om internationella avtal om social trygghet som medför skyldigheter att lämna personuppgifter till tredjeland.

En särskild bedömning av behovet av skyddsåtgärder

De lämpliga skyddsåtgärder som anges i artikel 46 befriar inte den personuppgifts-ansvariga från skyldigheten att göra en egen analys av de risker och det behov av skyddsåtgärder som en tredjelandsöverföring medför. Den personuppgiftsansvariga ska göra en TIA (Transfer Impact Assessment) för att säkerställa att personuppgifterna får ett lämpligt skydd i mottagarlandet. Detta inkluderar en analys av lagstiftningen i tredjelandet, särskilt myndigheters åtkomst till personuppgifter och möjligheten till effektiva rättsmedel för registrerade.

Kravet på en individuell bedömning av behovet av skyddsåtgärder vid tredjelands-överföringar med stöd av artikel 46 uppmärksammades av EU-domstolen i målet Schrems II.

Rättsfall
Max Schrems bestred, genom en domstolsprocess på Irland, Facebooks europeiska dotterbolag Facebook Irelands rätt att föra över hans personuppgifter till USA. I målet prövades lagligheten av de standardklausuler som använts som grund för överföringen till USA. EU-domstolen bedömde att standardklausulernas skydd var för svagt och att amerikanska myndigheter hade för generella möjligheter att få åtkomst till personuppgifter mot bakgrund av intressen som ”nationell säkerhet, allmänintresset och rättsefterlevnaden”. (EU-domstolens dom Schrems II, C-311/18, EU:C:2020:559)

EDPB har antagit rekommendationer om när ytterligare skyddsåtgärder kan behövas

och vad sådana åtgärder kan vara (EDPB:s rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter).

8.2 Undantag i särskilda situationer

Om det inte finns något beslut om adekvat skyddsnivå och inte heller några lämpliga skyddsåtgärder, kan vissa förhållanden ändå grunda rätt till överföring till tredjeland i särskilda situationer med stöd av artikel 49 i dataskyddsförordningen.

För Försäkringskassan kan det bli aktuellt att tillämpa artikel 49.1 d som tillåter överföring till ett tredjeland när den är nödvändig av viktiga skäl som rör allmänintresset. Allmänintresset ska vara erkänt i unionsrätten eller i den nationella rätt som den personuppgiftsansvariga omfattas av (artikel 49.4 i dataskyddsförordningen). Av skäl 112 till dataskyddsförordningen framgår att internationella utbyten av uppgifter mellan socialförsäkringsmyndigheter är en uppgiftsöverföring som krävs och är nödvändig med hänsyn till viktiga allmänintressen.

8.3 Särskilt om extraterritoriell lagstiftning

Extraterritoriell lagstiftning är lagar och regler som antas av en stat eller jurisdiktion och ska tillämpas utanför dess egna territoriella gränser. Sådan lagstiftning kan skapa juridiska konflikter, särskilt när den strider mot andra staters suveränitet eller lagar.

USA, Kina och Ryssland är exempel på länder med extraterritoriell lagstiftning som kan påverka dataskyddet. Företag med ett amerikanskt moderbolag kan till exempel vara tvungna att följa viss amerikansk lagstiftning oavsett var i världen företaget befinner sig. Det innebär att personuppgifter kan komma att föras ut ur EU och in i USA med stöd av amerikansk lagstiftning trots att företaget har sin verksamhet och sitt säte inom EU och trots att personuppgifterna enligt avtal ska behandlas inom EU.

Att personuppgifter överförs till ett företag inom EU som har ett amerikanskt eller kinesiskt moderbolag innebär inte att uppgifterna också anses överförda till tredjeland. Det är först när personuppgifterna faktiskt har överförts till USA eller Kina som en tredjelandsöverföring har skett. Däremot medför det en *risk* för att personuppgifter otillåtet kan komma att föras över till tredjeland. Vi måste därför vara mycket försiktiga i situationer där extraterritoriell lagstiftning kan komma att göras gällande på personuppgifter som Försäkringskassan har överfört till en extern part.

9 Säkerhet vid personuppgiftsbehandling

Artikel 32.1 i dataskyddsförordningen
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.

Försäkringskassan ansvarar i egenskap av personuppgiftsansvarig för att genomföra lämpliga tekniska och organisatoriska åtgärder för att dels säkerställa att behandlingen sker i enlighet med dataskyddsförordningen, dels kunna visa att så sker (artiklarna 5.2, 24.1 och 32.1 i dataskyddsförordningen). Vi behöver kunna bevisa att personuppgifterna behandlas på ett sätt som säkerställer lämplig säkerhet för dem.

Ansvaret för säkerheten sträcker sig lika långt som personuppgiftsansvaret. Det innebär att Försäkringskassan kan ha ansvar för säkerheten för personuppgifter även när vi inte har åtkomst till uppgifterna.

Rättsfall
I fråga om elektroniska självbetjäningstjänster i form av anmälan av tillfällig föräldrapenning via sms och arbetsgivares anmälan av sjukfall via en så kallad Infratjänst har HFD ansett att Försäkringskassan ska anses personuppgiftsansvarig för behandling som sker innan uppgifterna blir tillgängliga för myndigheten. HFD ansåg att Försäkringskassan därmed var skyldig att redovisa säkerheten vid behandlingen av personuppgifter trots att en sådan redovisning möjligen kunde komma att vara ofullständig i vissa hänseenden när det gällde säkerheten för personuppgifter hos operatörer eller avsändare. (HFD 2012 ref. 21).

Försäkringskassan ska vidta tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

Artikel 32.2 i dataskyddsförordningen
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.

De risker som avses i artikeln gäller intrång i de rättigheter och friheter som följer av EU:s stadga om de grundläggande rättigheterna. Det handlar särskilt om skyddet för personuppgifter, men dataskyddsförordningen avser även att skydda rätten till privat- och familjeliv, bostad och kommunikationer, tankefrihet, samvetsfrihet och religionsfrihet, yttrande- och informationsfrihet, näringsfrihet, rätten till ett effektivt rättsmedel och en opartisk domstol samt kulturell, religiös och språklig mångfald (skäl 2 och 4 till dataskyddsförordningen).

De skador som riskerna avser kan vara *fysiska*, *materiella* (skador på egendom) eller *immateriella* (till exempel lidande eller kränkning). Vi bör enligt skäl 75 till dataskyddsförordningen vara särskilt uppmärksamma på risker 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
- registrerade kan berövas sina rättigheter och friheter eller hindras från att utöva kontroll över sina personuppgifter
- behandlingen omfattar känsliga personuppgifter eller uppgifter om lagöverträdelser
- behandlingen medför bedömning av personliga aspekter, 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 (profilering)
- behandlingen omfattar personuppgifter rörande sårbara fysiska personer, framför allt barn
- behandlingen omfattar ett stort antal personuppgifter och gäller ett stort antal registrerade.

På Försäkringskassan ska risker för informationstillgångar identifieras och hanteras med avseende på konfidentialitet, riktighet, tillgänglighet och spårbarhet (*Försäkringskassans säkerhetspolicy* [2003:4]). Detta är ett sätt att som personuppgiftsansvarig agera i enlighet med det som anges i skäl 75 till dataskyddsförordningen.

9.1 Säkerhetsåtgärder

Vad som anses som lämpliga säkerhetsåtgärder exemplifieras direkt i artikel 32.1 och skäl 78 till dataskyddsförordningen. Det handlar bland annat om pseudonymisering, kryptering, tekniska åtgärder, säkerhetskopiering och system eller processer för att löpande följa upp säkerhetsåtgärderna.

Försäkringskassan är också skyldig att se till att medarbetarna känner till vad som gäller i fråga om behandling av personuppgifter (artiklarna 29 och 32.4 i dataskyddsförordningen).

Vi ska också löpande se över behovet av säkerhetsåtgärder och uppdatera dem när det behövs (artikel 24.1 i dataskyddsförordningen).

Det finns bestämmelser om säkerhetsåtgärder även i andra lagar och förordningar. Krav på informationssäkerhet finns ibland annat säkerhetsskyddslagen (2018:585) och förordningen (2022:524) om statliga myndigheters beredskap.

Läs mer
Du kan läsa mer om säkerhetsåtgärder på Försäkringskassan i Försäkringskassans säkerhetspolicy (2003:4), Försäkringskassans riktlinjer (2018:13) *Säkerhetsregler*, Försäkringskassans anvisningar (2025:17) *Säkerhetsskydd* och Försäkringskassans anvisningar (2022:09) *Säkerhet på Försäkringskassan*.

9.1.1 Pseudonymisering och kryptering

Artikel 4.5 i dataskyddsförordningen
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,

Pseudonymisering återkommer på flera ställen i dataskyddsförordningen som ett exempel på en lämplig teknisk och organisatorisk åtgärd (se artiklarna 6.4 e, 25.1, 32.1 a, 40.2 d och 89 i dataskyddsförordningen). Syftet med pseudonymisering är att minska möjligheten att koppla uppgifter till en fysisk person och därigenom skydda den personliga integriteten.

Vid pseudonymisering delas uppgifter om en fysisk person upp i åtskilda delar. Det innebär att det genom pseudonymisering inte längre går att hänföra uppgifterna till en fysisk person utan att kompletterande uppgifter används. De kompletterande uppgifterna ska förvaras separat och vara föremål för tekniska och organisatoriska åtgärder som säkerställer att det inte är möjligt att identifiera den registrerade.

Personuppgifter som har pseudonymiserats upphör inte att vara personuppgifter (skäl 26 till dataskyddsförordningen). Samtliga regler som gäller behandling av personuppgifter gäller alltså även dessa uppgifter. Om den personuppgiftsansvarige lämnar ut uppgifterna kan de dock upphöra att vara personuppgifter hos mottagaren om risken för identifiering i praktiken är försumbar för att identifiering är förbjuden i lag eller omöjlig att genomföra i praktiken (jfr EU-domstolens dom EDPS v SRB C-413/23 P, EU:C:2025:645). Kodnyckelförfaranden är en form av pseudonymisering där det inte finns något samband mellan de identifierande uppgifterna och pseudonymen. I stället väljs varje pseudonym som ett slumpvärde eller liknande. Kopplingen mellan de identifierande uppgifterna och pseudonymen sparas i en förteckning (kodnyckel). (Prop. 2017/18:298 s. 64)

Läs mer
Du kan läsa mer om pseudonymisering av personuppgifter i eSams vägledning (ES2022-01) *Pseudonymisering av personuppgifter*.

Om sekretess gäller för uppgifter om enskilda i en verksamhet där pseudonymisering används, skyddas även kodnyckeln av sekretess (18 kap. 9 § OSL). Läs mer om detta i vägledningen (2001:3) *Offentlighet, sekretess och utlämnande av handlingar och uppgifter*.

Kryptering är en process där en matematisk algoritm omvandlar data från ett läsbart till ett krypterat och oläsligt format. I och med detta kan bara de som har tillgång till rätt krypteringsnyckel läsa informationen.

9.1.2 Tillgång till personuppgifter

114 kap. 13 § första stycket SFB
Tillgången till personuppgifter ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter.

2 § förordningen om behandling av personuppgifter vid Försäkringskassan och Pensionsmyndigheten
Försäkringskassan och Pensionsmyndigheten ansvarar för att det inom respektive myndighet finns rutiner för att tilldela, förändra, ta bort och regelbundet följa upp behörigheter för tillgång till personuppgifter.

Av kravet på att tillgången till personuppgifter ska begränsas till vad den enskilda medarbetaren behöver för att fullgöra sina arbetsuppgifter följer indirekt att Försäkringskassan måste upprätta ett system för fördelning av behörigheter. Ett sådant system måste innehålla en funktionalitet som identifierar både vem som har en viss behörighet och vad behörigheten omfattar för att det ska fylla sitt syfte. (Prop. 2023/24:29 s. 71)

Ett system för fördelning av behörigheter förutsätter att Försäkringskassan aktivt tar ställning till vilket informationsbehov ett tjänsteåliggande eller uppdrag medför och att nödvändig behörighet tilldelas utifrån det (jämför prop. 2023/24:29 s. 72).

En behörighet definierar vilka uppgifter en användare har tillgång till och vad medarbetaren kan göra med uppgifterna. Det är medarbetarens arbetsuppgifter som sätter gränserna för den egentliga behörigheten. Den tekniska behörigheten – den faktiska möjligheten till åtkomst till personuppgifter – kan överstiga den rättsliga behörigheten att ta del av uppgifter. Medarbetaren får dock endast ta del av den information som hen behöver för att utföra sitt arbete.

Rättsfall
Kammarrätten i Stockholm har i ett mål om sanktionsavgift enligt dataskydds-förordningen bedömt att det har varit fråga om överträdelser av hög svårighetsgrad, när det har funnits möjlighet att ta del av information i den så kallade Skolplattformen utan behörighet. Informationen omfattade känsliga personuppgifter och även andra särskilt skyddsvärda uppgifter, till exempel skyddade personuppgifter och uppgifter om elevomdömen. Behandlingen berörde ett mycket stort antal registrerade, till stor del barn. De registrerade eleverna kunde inte påverka behandlingen. Omständigheten att skadan för de registrerade var relativt begränsad medförde ingen annan bedömning. (KRNS 7837-21)

9.1.3 Loggning

114 kap. 13 § andra stycket SFB
Åtkomsten till personuppgifter ska kontrolleras och följas upp regelbundet.

3 § förordningen om behandling av personuppgifter vid Försäkringskassan och Pensionsmyndigheten
Försäkringskassan och Pensionsmyndigheten ansvarar för att det inom respektive myndighet finns rutiner för att regelbundet kontrollera och följa upp åtkomsten till personuppgifter.

Kontroll och uppföljning av åtkomsten till personuppgifter förutsätter loggning. Loggning är en teknisk funktion, som innebär att behandlingshistorik sparas under en viss tid. Loggningen sker automatiskt i systemen och ska vara skyddad mot obehörig åtkomst och förändring.

Med uttrycket ”regelbundet” avses att kontroll och uppföljning ska göras systematiskt och inte bara om vi har fått anledning att misstänka att obehörig åtkomst har förekommit.

9.1.4 Inbyggt dataskydd och dataskydd som standard

Artikel 25.1 i dataskyddsförordningen

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.

Artikel 25.2 i dataskyddsförordningen

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.

Inbyggt dataskydd innebär att behovet av säkerhetsåtgärder ska beaktas redan när it-system och rutiner utvecklas. På så sätt ska åtgärderna vara en del av kravställningen vid design och utveckling och sedan naturligt komma till uttryck vid användning och slutligen eventuell avveckling av ett it-system.

Dataskydd som standard kan sägas innebära att arbetsflödena i ett system automatiskt ska styra användaren mot ett integritetssäkert arbetssätt och att grundinställningarna ska vara satta så att inte mer information än nödvändigt samlas in eller visas (prop. 2017/18:232 s. 174).

Läs mer

Mer information om dataskydd som standard finns i EDPB:s riktlinjer (4/2019) *Inbyggt dataskydd och dataskydd som standard*.

10 Personuppgiftsbiträdesavtal

När Försäkringskassan *anlitar* ett personuppgiftsbiträde eller *anlitas* som personuppgiftsbiträde behöver vi ingå ett personuppgiftsbiträdesavtal.

Ett personuppgiftsbiträdesavtal reglerar behandling av personuppgifter och ska bland annat säkerställa att både den personuppgiftsansvariga och biträdet

- följer dataskyddsförordningen
- är medvetna om sina åtaganden och skyldigheter mot varandra och mot de registrerade
- skyddar kunders, medarbetares och andra kategorier av registrerades personuppgifter
- dokumenterar tydligt och därmed enkelt kan visa att de följer reglerna (ansvarsskyldighet).

Personuppgiftsbiträdesavtalet ska vara bindande för personuppgiftsbiträdet gentemot den personuppgiftsansvariga (artikel 28.3 i dataskyddsförordningen).

Avtalet måste vara skriftligt (artikel 28.9 i dataskyddsförordningen).

Läs mer

Du kan läsa mer om personuppgiftsbiträdesavtal i Försäkringskassans riktlinjer (2019:01) *Personuppgiftsbiträdesavtal*. Där beskrivs bland annat förutsättningar för att teckna ett sådant avtal, vad som ska ingå i det och vilken Wimimall som ska användas.

10.1 När behöver vi ett personuppgiftsbiträdesavtal?

Artikel 28.3 i dataskyddsförordningen

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.

Försäkringskassan behöver ett personuppgiftsbiträdesavtal när vi ska anlita en utomstående aktör för att behandla personuppgifter för vår räkning. Försäkringskassan är då personuppgiftsansvarig och den utomstående aktören är personuppgiftsbiträde. En utomstående aktör kan till exempel vara en annan myndighet eller en enskild leverantör av tjänster. Ett exempel på personuppgiftsbiträde är leverantörer av it-tjänster, såsom rekryteringsverktyg.

Försäkringskassan behöver också ett personuppgiftsbiträdesavtal när vi anlitas av en utomstående aktör för att behandla personuppgifter för den aktörens räkning. Försäkringskassan är då personuppgiftsbiträde och den utomstående aktören är personuppgiftsansvarig. Det kan till exempel vara när vi tillhandahåller it-driftstjänster åt andra myndigheter.

10.2 Vad ska ett personuppgiftsbiträdesavtal innehålla?

I artikel 28.3 i dataskyddsförordningen anges vad ett personuppgiftsbiträdesavtal ska innehålla. Vi kan skriva in fler krav, men vi kan inte utelämna något av dem som anges i artikeln.

Personuppgiftsbiträdesavtalet bör innehålla specifik och konkret information om hur kraven kommer att uppfyllas och vilken säkerhetsnivå som krävs för personuppgifts-behandlingen. Det ska alltså inte bara upprepa vad som står i dataskyddsförordningen (EDPB:s riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, s. 37).

10.2.1 Information om behandlingen, personuppgifterna, de registrerade och den personuppgiftsansvarigas skyldigheter och rättigheter

Artikel 28.3 första meningen i dataskyddsförordningen

När uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett avtal […] i vilken föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter anges.

Bestämmelsen förtydligas i EDPB:s riktlinjer angående begreppen personuppgiftsansvarig och personuppgiftsbiträde, s. 37 och 38:

- **Föremålet för behandlingen** måste specificeras så att det är tydligt vad som är det centrala syftet med behandlingen. När det gäller behandlingens *varaktighet* kan den exakta tidsperioden eller de kriterier som används för att fastställa den exakta tidsperioden anges. Ett annat sätt att ange varaktigheten kan vara att hänvisa till huvudavtalets längd (EDPB:s riktlinjer angående begreppen personuppgiftsansvarig och personuppgiftsbiträde, s. 37 f.).
- Med **behandlingens art** avses hur personuppgifter hanteras i praktiken, det vill säga vilka åtgärder som vidtas för att uppnå ändamålet. Behandlingens *ändamål* beskriver varför personuppgifterna behandlas och vilket mål eller behov som ska uppfyllas. Beskrivningen av behandlingens art och ändamål bör vara så omfattande som möjligt, så att externa parter (till exempel tillsynsmyndigheter) kan förstå innehållet och riskerna med behandlingen (EDPB:s riktlinjer angående begreppen personuppgiftsansvarig och personuppgiftsbiträde, s. 38).
- **Typen av personuppgifter** bör specificeras så detaljerat som möjligt för att underlätta förståelse för en extern part. Det är exempelvis inte tillräckligt att endast ange ”personuppgifter” eller ”särskilda kategorier av personuppgifter”. Även **kategorier av registrerade** bör anges på ett specifikt sätt (EDPB:s riktlinjer angående begreppen personuppgiftsansvarig och personuppgiftsbiträde, s. 38).
- Med **den personuppgiftsansvarigas skyldigheter** avses till exempel skyldigheten att:
  - tillhandahålla personuppgiftsbiträdet de uppgifter som nämns i avtalet
  - tillhandahålla och dokumentera alla instruktioner för behandlingen
  - säkerställa att personuppgiftsbiträdet följer dataskyddsförordningen
  - övervaka behandlingen, till exempel genom revisioner och inspektioner.

- Med **den personuppgiftsansvarigas rättigheter** avses till exempel den personuppgiftsansvarigas rätt att utföra inspektioner och revisioner (EDPB:s riktlinjer angående begreppen personuppgiftsansvarig och personuppgiftsbiträde s. 38).

10.2.2 Dokumenterade instruktioner från den personuppgiftsansvariga

Artikel 28.3 a) i dataskyddsförordningen

I det avtalet […] 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,

Personuppgiftsbiträdet får bara behandla personuppgifterna enligt den personuppgiftsansvarigas instruktioner, som ska framgå av personuppgiftsbiträdesavtalet. Det innebär att det är den personuppgiftsansvariga, och inte personuppgiftsbiträdet, som bestämmer varför och hur personuppgifterna ska behandlas. Om personuppgiftsbiträdet frångår instruktionerna och själv fastställer ändamålen och medlen för personuppgiftsbehandlingen, kan personuppgiftsbiträdet anses vara personuppgiftsansvarig för behandlingen (artikel 28.10 i dataskyddsförordningen).

Artikel 28 ska inte tillämpas om det skulle strida mot TF eller YGL (1 kap. 7 § första stycket dataskyddslagen). När Försäkringskassan är personuppgiftsbiträde kan vi i avtalet reservera oss för de skyldigheter som följer av tryckfrihetsförordningen och yttrandefrihetsgrundlagen (Öman, *Dataskyddsförordningen [GDPR] m.m. En kommentar*, JUNO Version 4, kommentaren till artikel 28). Det kan till exempel handla om Försäkringskassans skyldighet att lämna ut offentliga allmänna handlingar enligt 2 kap. TF eller om de anställdas rätt att lämna uppgifter enligt reglerna om meddelandefrihet i YGL.

Läs mer

Du kan läsa mer om handlingsoffentligheten och meddelandefriheten i Försäkringskassans vägledning 2001:3 *Offentlighet, sekretess och utlämnande av handlingar och uppgifter*.

10.2.3 Konfidentialitet eller lagstadgad tystnadsplikt

Artikel 28.3 b i dataskyddsförordningen

I det avtalet […] ska det särskilt föreskrivas att personuppgiftsbiträdet […]

b) säkerställer att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt,

Personuppgiftsbiträdet ska säkerställa att personer som behandlar uppgifterna har tystnadsplikt. Detta avtalsvillkor ska täcka biträdets anställda, konsulter och all annan personal som under biträdets överinseende behandlar uppgifterna. Tystnadsplikten kan följa av ett avtal eller av gällande rätt.

När Försäkringskassan anlitar en annan myndighet för teknisk bearbetning eller teknisk lagring finns sekretessbestämmelser i OSL. OSL gäller också när Försäkringskassan agerar personuppgiftsbiträde åt en annan myndighet eller åt en enskild.

Läs mer

Läs mer om tillämpliga sekretessbestämmelser i Försäkringskassans vägledning (2001:3) *Offentlighet, sekretess och utlämnande av handlingar och uppgifter*.

När Försäkringskassan uppdrar åt ett företag eller en annan enskild (tjänsteleverantör) att endast tekniskt bearbeta eller tekniskt lagra uppgifter gäller lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller teknisk lagring av uppgifter. Lagen innebär en tystnadsplikt för de anställda som deltar eller har deltagit i tjänsteleverantörens verksamhet på uppdrag av Försäkringskassan.

Personuppgiftsbiträdesavtalet behöver inte införa en “ny” tystnadsplikt för biträdet, men bör hänvisa till tillämplig bestämmelse.

10.2.4 Säkerhetsåtgärder

Artikel 28.3 c i dataskyddsförordningen

I det avtalet […] ska det särskilt föreskrivas att personuppgiftsbiträdet […]

c) ska vidta alla åtgärder som krävs enligt artikel 32,

Enligt artikel 32 i dataskyddsförordningen ska personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå i förhållande till riskerna för fysiska personers rättigheter och friheter. Även om denna skyldighet framgår av artikel 32 måste den också framgå av avtalet.

Avtalet ska dock inte enbart hänvisa till eller återupprepa artikel 32, utan måste innehålla eller hänvisa till information om de säkerhetsåtgärder som personuppgifts-biträdet ska vidta. Avtalet ska också innehålla en skyldighet för personuppgiftsbiträdet att inte göra några ändringar utan den personuppgiftsansvarigas godkännande. Det ska också göras en regelbunden översyn av säkerhetsåtgärderna för att säkerställa att de är lämpliga över tid. Hur detaljerade instruktionerna behöver vara beror på omständigheterna i det enskilda fallet. (EDPB:s riktlinjer angående begreppen personuppgiftsansvarig och personuppgiftsbiträde, s. 40)

Du kan läsa mer om säkerhetsåtgärder i avsnitt 9.1.

10.2.5 Underbiträden

Artikel 28.3 d i dataskyddsförordningen
I det avtalet […] ska det särskilt föreskrivas att personuppgiftsbiträdet […]
d) ska respektera de villkor som avses i punkterna 2 och 4 för anlitandet av ett annat personuppgiftsbiträde,

Artikel 28.4 i dataskyddsförordningen
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.

Ibland kan ett personuppgiftsbiträde anlita en utomstående aktör för att utföra en specifik behandling på den personuppgiftsansvarigas vägnar. En sådan aktör kallas underbiträde. Personuppgiftsbiträdet och underbiträdet behöver då ingå ett avtal där underbiträdet åläggs samma skyldigheter som personuppgiftsbiträdet har i förhållande till den personuppgiftsansvariga.

Enligt artikel 28.3 d i dataskyddsförordningen ska det i personuppgiftsbiträdesavtalet föreskrivas att personuppgiftsbiträdet ska respektera följande villkor:

- Personuppgiftsbiträdet får inte anlita ett underbiträde utan ett särskilt eller allmänt skriftligt förhandstillstånd från den personuppgiftsansvariga (artikel 28.2 första meningen i dataskyddsförordningen).
- Om personuppgiftsbiträdet har fått ett allmänt förhandstillstånd, ska personuppgiftsbiträdet informera den personuppgiftsansvariga om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden, så att den personuppgiftsansvariga har möjlighet att invända mot det (artikel 28.2 andra meningen i dataskyddsförordningen).
- Om personuppgiftsbiträdet anlitar ett underbiträde ska underbiträdet, genom ett avtal eller en annan rättsakt, åläggas samma skyldigheter som personuppgiftsbiträdet har i förhållande till den personuppgiftsansvariga. Underbiträdet måste framför allt ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i dataskyddsförordningen (artikel 28.4 första meningen i dataskyddsförordningen). Detta avtal behöver inte vara precis likadant som avtalet mellan den personuppgiftsansvariga och personuppgiftsbiträdet. Skyldigheterna måste dock vara desamma.

Det framgår inte av dataskyddsförordningen vad som händer om den personuppgifts-ansvariga har invändningar mot att ett personuppgiftsbiträde anlitar eller ersätter ett underbiträde. Det kan dock regleras i biträdesavtalet. Vi kan till exempel skriva att personuppgiftsbiträdet inte får anlita ett underbiträde som vi invänder mot.

10.2.6 De registrerades rättigheter

Artikel 28.3 e i dataskyddsförordningen

I det avtalet […] ska det särskilt föreskrivas att personuppgiftsbiträdet […]

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,

Det ska framgå av personuppgiftsbiträdesavtalet att personuppgiftsbiträdet genom lämpliga tekniska och organisatoriska åtgärder ska hjälpa den personuppgiftsansvariga att fullgöra sina skyldigheter gentemot de registrerade. Skyldigheten att hjälpa den personuppgiftsansvariga bör specificeras så att det tydligt framgår vilken slags hjälp personuppgiftsbiträdet ska bistå med (EDPB:s riktlinjer angående begreppen personuppgiftsansvarig och personuppgiftsbiträde, s. 41).

Det är alltid den personuppgiftsansvariga som i slutändan är ansvarig för att fullgöra sina skyldigheter gentemot de registrerade, även om det i praktiken är ett personuppgiftsbiträde som hanterar begäran från de registrerade. Det är exempelvis inte godtagbart att lämna ut information om behandlingen eller ett registerutdrag senare av det skälet att personuppgifterna behandlas av ett personuppgiftsbiträde.

10.2.7 Bistå den personuppgiftsansvariga

Artikel 28.3 f i dataskyddsförordningen

I det avtalet […] ska det särskilt föreskrivas att personuppgiftsbiträdet […]

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,

Den personuppgiftsansvariga är enligt dataskyddsförordningen bland annat skyldig att

- säkerställa att personuppgifter behandlas på ett säkert sätt (artikel 32)
- anmäla personuppgiftsincidenter till tillsynsmyndigheten (artikel 33)
- informera den registrerade om en personuppgiftsincident (artikel 34)
- i förekommande fall göra konsekvensbedömningar och samråda med tillsynsmyndigheten (artikel 35 och 36).

Personuppgiftsbiträdesavtalet ska inte bara upprepa skyldigheterna som de anges i dataskyddsförordningen. I stället bör avtalet innehålla specificerade uppgifter om hur personuppgiftsbiträdet ska hjälpa den personuppgiftsansvariga att uppfylla skyldigheterna.

Den personuppgiftsansvariga är ytterst ansvarig för att säkerställa att skyldigheterna enligt artiklarna 32–36 i dataskyddsförordningen fullgörs, även om personuppgiftsbiträdet ska hjälpa till att göra det.

10.2.8 När behandlingsuppdraget upphör

Artikel 28.3 g i dataskyddsförordningen

I det avtalet […] ska det särskilt föreskrivas att personuppgiftsbiträdet […]

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,

Personuppgifter måste skyddas även efter att avtalsförhållandet mellan den personuppgiftsansvariga och personuppgiftsbiträde har upphört. Syftet med bestämmelsen är att säkerställa ett sådant skydd. Den personuppgiftsansvariga ska därför bestämma vad som ska hända med de personuppgifter som personuppgiftsbiträdet har behandlat.

Personuppgifterna ska gallras och återlämnas på ett säkert sätt. Personuppgiftsbiträdet behöver beakta bestämmelserna om säkerhetsåtgärder i artikel 32 i dataskydds-förordningen vid radering och återlämning.

Personuppgiftsbiträdet måste radera alla befintliga kopior av personuppgifterna, om inte EU-rätten eller medlemsstaternas nationella rätt kräver att personuppgifterna lagras. Det är den nationella rätt som personuppgiftsbiträdet omfattas av som avses (skäl 81 till dataskyddsförordningen).

10.2.9 Tillgång till information, granskning och inspektioner

Artikel 28.3 h i dataskyddsförordningen

I det avtalet […] ska det särskilt föreskrivas att personuppgiftsbiträdet […]

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.

Personuppgiftsbiträdet måste kunna visa för den personuppgiftsansvariga att biträdet följer alla bestämmelser i artikel 28 i dataskyddsförordningen. Avtalet behöver beskriva hur ofta och på vilket sätt personuppgiftsbiträdet ska informera den personuppgiftsansvariga, så att den personuppgiftsansvariga får fullständig information när det gäller detaljer om behandlingen som är relevanta för att kunna visa att skyldigheterna i artikel 28 efterlevs.

10.3 Standardavtalsklausuler

Artikel 28.6 i dataskyddsförordningen
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.

Artikel 28.7 i dataskyddsförordningen
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.

Artikel 28.8 i dataskyddsförordningen
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.

Både EU-kommissionen och medlemsstaternas dataskyddsmyndigheter får fastställa standardiserade avtalsklausuler som kan användas för att reglera förhållandet mellan personuppgiftsansvariga och personuppgiftsbiträden. EU-kommissionen har tagit fram standardavtalsklausuler för personuppgiftsansvariga och personuppgiftsbiträden i EU och EEA, Kommissionens genomförandebeslut (EU) 2021/915 av den 4 juni 2021 om standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden enligt artikel 28.7 i Europaparlamentets och rådets förordning (EU) 2016/679 och artikel 29.7 i Europaparlamentets och rådets förordning (EU) 2018/1725. Även den danska tillsynsmyndigheten har tagit fram standardavtalsklausuler för biträdessituationer. IMY har bestämt att de standardavtalsklausuler som den danska tillsynsmyndigheten har tagit fram kan användas av verksamheter i Sverige. Fler medlemsstater kan också komma att ta fram standardavtalsklausuler.

Vi måste inte använda standardavtalsklausulerna. Om vi inte kan använda Försäkringskassans mallar för personuppgiftsbiträdesavtal kan standardavtals-klausulerna dock vara till stor hjälp för att vi ska vara säkra på att ett avtal innehåller alla obligatoriska delar.

Om vi använder standardavtalsklausuler i våra personuppgiftsbiträdesavtal får klausulerna inte ändras. Vi måste också säkerställa att avtalen återspeglar de faktiska förhållandena mellan den personuppgiftsansvariga och personuppgiftsbiträdet och att instruktionerna till personuppgiftsbiträdet är korrekta. Vi kan lägga till ytterligare klausuler till standardavtalsklausulerna, men bara om de inte direkt eller indirekt strider mot standardavtalsklausulerna eller påverkar de registrerades grundläggande rättigheter och friheter (skäl 109 till dataskyddsförordningen).

Läs mer

Du kan läsa mer om EU-kommissionens standardavtalsklausuler på EU-kommissionens officiella webbplats. Där kan du också ladda ner standardavtalsklausulerna.

Du kan läsa mer om de standardavtalsklausuler som den danska tillsynsmyndigheten tagit fram på Datatilsynets webbplats. De danska standardavtalsklausulerna finns på alla officiella EU-språk på EDPB:s webbplats.

11 Rätten till information

Rätten till information är ett utflöde av den grundläggande principen om öppenhet i artikel 5 i dataskyddsförordningen. Rättigheten har även direkt koppling till principen om korrekthet, eftersom information och insyn anses bidra till en rättvis och öppen personuppgiftsbehandling för den registrerade. Läs mer om principerna i avsnitt 3.

Syftet med rätten till information framgår av skäl 39 till dataskyddsförordningen och Artikel 29-arbetsgruppens riktlinjer om öppenhet (WP260rev.01) punkterna 2 och 10. Syftet är att:

- skapa tillit för verksamheten
- ge registrerade möjlighet att i förväg bedöma syftet och konsekvensen av en personuppgiftsbehandling
- ge registrerade möjlighet att förstå och om så krävs bestrida personuppgiftsbehandlingar
- ge registrerade möjlighet att i övrigt utöva kontroll över sina personuppgifter och utöva sina dataskyddsrättsliga rättigheter.

Rätten till information för den registrerade innebär en skyldighet för den personuppgiftsansvariga att lämna information.

11.1 Rätten till information när personuppgifter samlas in från den registrerade

11.1.1 Vad ska vi informera om?

Artikel 13 i dataskyddsförordningen

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.

[…]

Kraven är delvis olika när vi samlar in personuppgifter direkt från den registrerade och när vi gör det från någon annan.

Vi samlar in personuppgifter från den registrerade genom att hen medvetet lämnar personuppgifter till oss, exempelvis genom att fylla i och skicka in en ansökan. Det räknas också som att personuppgifter samlas in från den registrerade när personuppgifter lämnas av en vårdnadshavare, ställföreträdare eller ombud med direkt uppdrag att lämna personuppgifterna (jämför Öman, *Dataskyddsförordningen [GDPR] m.m. En kommentar*, JUNO Version 4, kommentaren till artikel 13).

När vi samlar in personuppgifter direkt från den registrerade ska hen i vart fall få information om

- att Försäkringskassan är personuppgiftsansvarig
- Försäkringskassans kontaktuppgifter
- vårt dataskyddsombuds kontaktuppgifter
- ändamål och rättslig grund för aktuell personuppgiftsbehandling
- till vem vi eventuellt lämnar personuppgifterna

- vilka tredje länder eller internationella organisationer som vi överför personuppgifterna till och grund för överföringen
- hur länge vi sparar personuppgifterna
- sina rättigheter
- att hen kan återkalla sitt samtycke om den rättsliga grunden för behandlingen är samtycke
- att hen kan lämna klagomål till IMY
- om ett eventuellt krav att lämna personuppgifter är lagstadgat, avtalsenligt eller nödvändigt för att ingå ett avtal och de möjliga följderna av att uppgifterna inte lämnas
- eventuell förekomst av automatiserat beslutsfattande, inbegripet profilering.

Om det blir aktuellt att vidarebehandla insamlade personuppgifter för ett annat ändamål än det som uppgifterna ursprungligen samlats in för, kan vi behöva lämna ytterligare information (artikel 13.3 i dataskyddsförordningen).

Rättsfall

Kammarrätten i Stockholm har i ett mål om sanktionsavgift enligt dataskydds-förordningen bland annat bedömt om Klarna Bank AB har uppfyllt kravet på information enligt artikel 13. Bolaget lämnade information till de registrerade dels vid registrering för en tjänst och dels genom dataskyddsinformation på sin hemsida. Bolaget informerade om den rättsliga grunden för behandling av personuppgifter vid registrering för tjänsten, men inte på hemsidan, vilket bedömdes vara otillräckligt (artikel 13.1 c). Bolaget lämnade inte information om hur de registrerade kan få tillgång till information om skyddsåtgärder vid tredjelandsöverföringar (artikel 13.1 f). Bolaget lämnade inte fullständig information om lagring av uppgifter, vilket bland annat medförde att den registrerade inte kunde bedöma lagringstiden för särskilda uppgifter eller ändamål (artikel 13.2 a). Bolaget informerade inte heller om användningen av en scoremodell som bland annat byggde på intern och extern finansiell information, och vilka typer av uppgifter som ingick i den finansiella informationen (artikel 13.2 f). För bland annat dessa överträdelser påfördes bolaget sanktionsavgift. (KRNS mål nr 2829-23)

11.1.2 Undantag från skyldigheten att informera

Artikel 13.4 i dataskyddsförordningen

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

5 kap. 1 § första stycket dataskyddslagen

Artiklarna 13–15 i EU:s dataskyddsförordning om information och rätt att få tillgång till personuppgifter gäller inte sådana uppgifter som den personuppgiftsansvarige inte får lämna ut till den registrerade enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning.

Den registrerade får anses förfoga över informationen om det är klarlagt att hen har fått del av informationen och att den kan ge hen förståelse för vilka uppgifter som behandlas, vilka rättigheter hen har och hur hen kan gå tillväga för att utöva sina rättigheter.

Vi måste kunna visa att undantaget från informationsskyldigheten är uppfyllt. Det framgår av den grundläggande principen om ansvarsskyldighet (jämför artikel 5.1 a och 2 i dataskyddsförordningen, läs mer i avsnitt 3.7). Det innebär att vi måste kunna visa vilken information den registrerade har fått samt hur och när hen har fått informationen.

Informationsskyldigheten omfattar inte sådana uppgifter som den registrerade inte får ta del av på grund av bestämmelser om sekretess. Det kan till exempel handla om uppgifter som rör säkerhet i it-miljön (18 kap. 8 § OSL) eller uppgifter om metoder, modeller och riskfaktorer som hänför sig till dataanalyser och urval för att förebygga, förhindra och upptäcka felaktiga utbetalningar (17 kap. 1 b § OSL).

11.1.3 När ska vi informera?

Artikel 13.1 och 3 i dataskyddsförordningen

1.Om personuppgifter som rör en registrerad person samlas in från den registrerade, ska den personuppgiftsansvarige, när personuppgifterna erhålls, till den registrerade lämna information […]

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.

När vi samlar in personuppgifter från den registrerade ska vi informera hen vid den tidpunkt då vi får personuppgifterna. I praktiken kan det innebära att vi ständigt tillhandahåller aktuell information, exempelvis genom vår webbplats (se skäl 58 till dataskyddsförordningen).

Om insamlade personuppgifter ska vidarebehandlas för ett annat ändamål än det som uppgifterna ursprungligen samlades in för, ska vi informera den registrerade om det innan vidarebehandlingen påbörjas.

11.1.4 Hur ska vi informera?

Informationen ska vara koncis, klar och tydlig, begriplig och lätt tillgänglig. Vi ska också använda ett klart och tydligt språk. (Artikel 12.1 i dataskyddsförordningen)

Kravet på att informationen ska vara *koncis, klar och tydlig* betyder att vi bör presentera informationen på ett effektivt och kortfattat sätt och tydligt särskilja den från information som inte gäller integritet (Artikel 29-gruppens riktlinjer om öppenhet, punkt 8).

Att informationen ska vara *begriplig* betyder att den bör kunna förstås av en genomsnittsmedlem av den avsedda målgruppen (Artikel 29-gruppens riktlinjer om öppenhet, punkt 8).

Kravet på en *lätt tillgänglig form* är uppfyllt om det är direkt uppenbart för den registrerade var och hur hen kan hitta informationen, exempelvis genom att hen får informationen direkt, genom en länk, genom tydlig vägledning eller som ett svar på en fråga (Artikel 29-gruppens riktlinjer om öppenhet, punkt 11).

Att informationen ska lämnas på ett *klart och tydligt språk* betyder att informationen bör ges på ett så enkelt sätt som möjligt. Framför allt bör syftena med och de rättsliga grunderna för behandlingen av personuppgifterna vara tydliga (Artikel 29-gruppens riktlinjer om öppenhet, punkt 13).

Läs mer
Du kan läsa mer om att skriva begripligt och om klarspråk på intranätet Fia. Sök på ”klarspråk”.

Läs också gärna Myndigheternas skrivregler, som ges ut av Språkrådet.

När mottagaren av informationen är ett barn eller någon annan utsatt person krävs särskild hänsyn vid utformningen av informationen eller kommunikationen (artikel 12.1 i dataskyddsförordningen). Barn förtjänar särskilt skydd och all information och kommunikation som riktas till barn bör utformas med ett tydligt och enkelt språk som barnet lätt kan förstå (skäl 58). Vi bör säkerställa att orden, tonen och stilen i det språk som används är lämpligt och anpassat för barn, så att de barn som får informationen förstår att den är riktad till dem (Artikel 29-gruppens riktlinjer om öppenhet, punkt 14).

När vi informerar bör vi vidta någon form av aktiv åtgärd eller aktivt ledsaga den registrerade till den plats där informationen finns, exempelvis genom att i en e-tjänst ha en direktlänk till forsakringskassan.se med all obligatorisk information. Den registrerade ska inte behöva leta rätt på informationen bland annan information (jämför Artikel 29-gruppens riktlinjer om öppenhet, punkt 33).

Vi kan också uppfylla vår informationsskyldighet genom en *skiktad metod* (se EU-domstolens dom den 18 december 2025, Integritetsskyddsmyndigheten mot AB Storstockholms Lokaltrafik, C-422/24, punkt 42). Det innebär att vi lämnar information i olika lager eller skikt, först med viss grundläggande information och sedan en hänvisning till var den registrerade kan ta del av mer detaljerad och fullständig information.

11.2 Rätten till information när vi inte fått personuppgifter från den registrerade

11.2.1 Vad ska vi informera om?

Artikel 14 i dataskyddsförordningen
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.

Att personuppgifterna inte samlas in från den registrerade innebär att uppgifterna samlas in från andra källor. Alla personuppgifter som inte kommer från den registrerade omfattas av tillämpningsområdet för artikel 14 (EU-domstolens dom Másdi, C-169/23, EU:C:2024:988, punkt 49).

Det kan vara aktuellt att lämna information enligt artikel 14 när vi samlar in personuppgifter från exempelvis myndigheter, arbetsgivare, vårdgivare, banker eller försäkringsbolag.

Den information som ska lämnas enligt artikel 14 är samma information som när personuppgifter samlas in från den registrerade (se avsnitt 11.1.1). Därutöver ska vi även informera om

- de kategorier av personuppgifter som behandlingen gäller
- varifrån personuppgifterna kommer och i förekommande fall om vi har hämtat dem från allmänt tillgängliga källor.

11.2.2 Undantag från skyldigheten att informera

Artikel 14.5 i dataskyddsförordningen
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.

Vi måste kunna visa att undantaget från informationsskyldigheten är uppfyllt. Det framgår av den grundläggande principen om ansvarsskyldighet (artikel 5.1 a och 2 i dataskyddsförordningen, läs mer i avsnitt 3.7). Det kan till exempel innebära att vi måste kunna visa vilken information den registrerade har fått, hur och när hen har fått den och att vi har vidtagit lämpliga åtgärder. Det kan alltså krävas viss dokumentation.

Den registrerade har redan tillgång till informationen

Vi behöver inte informera den registrerade om hen redan har tillgång till informationen. Det behöver i så fall vara klarlagt att hen har fått del av informationen och kan förstå vilka uppgifter som behandlas, vilka rättigheter hen har och hur hen kan gå tillväga för att utöva sina rättigheter.

Det är omöjligt eller innebär en oproportionell ansträngning att informera

Vi behöver inte informera den registrerade om det skulle visa sig vara omöjligt eller innebära en oproportionell ansträngning.

Omöjligheten eller den oproportionella ansträngningen måste ha direkt koppling till omständigheten att vi har fått personuppgifterna från någon annan än den registrerade. Det kan handla om att det är omöjligt att få tag på kontaktuppgifter till den registrerade, till exempel för att den registrerade har en okänd adress i utlandet (Artikel 29-gruppens riktlinjer om öppenhet, punkt 59).

Det kan vara fråga om en oproportionell ansträngning om den arbetsinsats som krävs för att informera är orimligt ansträngande. Vid bedömningen av om det rör sig om en oproportionell ansträngning ska antalet registrerade, uppgifternas ålder och lämpliga skyddsåtgärder särskilt beaktas. (Skäl 62 till dataskyddsförordningen)

Det krävs en helhetsbedömning av samtliga relevanta omständigheter. Proportionaliteten får bedömas i förhållande till den ansträngning det innebär att informera, arten av personuppgifter som ska behandlas, behandlingens ändamål, de särskilda integritetsrisker som kan vara förknippade med behandlingen och det intresse de registrerade kan antas ha av att bli informerade om behandlingen. Vi behöver som regel informera de registrerade om vi ska behandla känsliga personuppgifter, även om det innebär ett förhållandevis stort besvär. Behandlingar för att kontrollera personuppgifter som de registrerade lämnat om till exempel inkomst lär också som regel kräva information. Kan det antas att de registrerade skulle bli överraskade av att få veta att vi håller på med en viss behandling av personuppgifter, lär vidare information som regel behöva lämnas. (se Öman, *Dataskyddsförordningen [GDPR] m.m. En kommentar*, JUNO Version 4, kommentaren till artikel 14)

Om undantaget ska tillämpas måste vi vidta lämpliga åtgärder för att skydda den registrerades rättigheter, friheter och berättigade intressen. Lämpliga åtgärder kan vara att offentliggöra informationen, till exempel genom att lägga ut den på vår webbplats, ha flera hänvisningar till vår webbplats och aktivt informera genom olika nyhetskanaler (Artikel 29-gruppens riktlinjer om öppenhet, punkt 64).

Informationen gör det sannolikt omöjligt eller avsevärt svårare att uppfylla målen med behandlingen

Vi behöver inte informera den registrerade om det sannolikt kommer att göra det omöjligt eller avsevärt svårare att uppfylla målen med personuppgiftsbehandlingen.

Om undantaget ska tillämpas måste vi vidta lämpliga åtgärder för att skydda den registrerades rättigheter, friheter och berättigade intressen. Lämpliga åtgärder kan vara att offentliggöra informationen, till exempel genom att lägga ut den på vår webbplats, ha flera hänvisningar till vår webbplats och aktivt informera genom olika nyhetskanaler (Artikel 29-gruppens riktlinjer om öppenhet, punkt 64).

När det uttryckligen föreskrivits om insamlande och utlämnande av uppgifter i nationell rätt

Vi behöver inte informera den registrerade om det finns uttryckliga föreskrifter om att få eller lämna uppgifter i svensk rätt. Det måste då även i svensk rätt finnas uttryckliga föreskrifter om lämpliga åtgärder för att skydda den registrerades berättigade intressen.

Det är inte helt tydligt vad som krävs för att det ska anses vara ”uttryckliga föreskrifter”. Enligt regeringen innebär det att det ska finnas föreskrifter om en rätt att få uppgifter eller föreskrifter om en uppgiftsskyldighet. Regeringen har bland annat ansett att bestämmelserna om rätten att ta del av allmänna handlingar i TF och uppgiftsskyldigheterna i 6 kap. 4 och 5 §§ OSL är sådana nationella föreskrifter som uppfyller kravet på uttryckliga föreskrifter som avses i artikel 14.5 c (prop. 2017/18:298 s. 110 ff.).

EDPB anser att de uttryckliga föreskrifterna i nationell rätt direkt ska avse den personuppgiftsansvariga och innehålla ett obligatoriskt krav i fråga om att få eller lämna uppgifter. ”Lämpliga åtgärder för att skydda den registrerades berättigade intressen” ska enligt EDPB fastställas i samma författning som föreskrifterna om krav på att få eller lämna uppgifter (Artikel 29-arbetsgruppens riktlinjer om öppenhet, punkt 66).

Enligt EU-domstolen ska de nationella bestämmelser som föreskriver om att få eller att lämna personuppgifterna vara tillräckligt fullständiga och bindande. Bestämmelserna ska ge den registrerade tillräcklig information om vilka personuppgifter som samlas in eller lämnas ut och om personuppgiftsbehandlingen så att hen kan utöva kontroll över sina personuppgifter och utöva sina rättigheter enligt dataskyddsförordningen. Skyddsnivån för den registrerade ska bli åtminstone likvärdig med den som garanteras

om vi hade gett den registrerade information enligt artikel 14 (EU-domstolens dom Másdi, C-169/23, EU:C:2024:988, skäl 44 och 52 ff.).

Undantag vid sekretess

Informationsskyldigheten omfattar inte sådana uppgifter som den enskilde inte får ta del av på grund av bestämmelser om sekretess (5 kap. 1 § dataskyddslagen). Det kan till exempel handla om uppgifter om metoder, modeller och riskfaktorer som hänför sig till dataanalyser och urval för att förebygga, förhindra och upptäcka felaktiga utbetalningar (17 kap. 1 b § OSL) och uppgift som hänför sig till förundersökning i brottmål (18 kap 1 § OSL).

11.2.3 När ska vi informera?

Artikel 14.3 och 4 i dataskyddsförordningen

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.

Som huvudregel ska den registrerade få information om personuppgiftsbehandlingen senast inom en månad efter att personuppgifter har samlats in från någon annan än hen. Vissa undantag från huvudregeln finns i artikel 14.3 b och c.

Ett förutsett utlämnande till en annan mottagare kan till exempel vara att lämna ut uppgifter till ett personuppgiftsbiträde eller att lämna ut uppgifter på grund av en reglerad uppgiftsskyldighet.

Om vi ska vidarebehandla insamlade personuppgifter för ett annat ändamål än det som uppgifterna ursprungligen samlades in för, ska vi informera om det innan vidarebehandlingen påbörjas.

11.2.4 Hur ska vi informera?

I avsnitt 11.1.4 anges vad som gäller när vi lämnar informationen och hur den bör vara utformad.

Om den registrerade inte själv kan läsa och förstå informationen eller ta tillvara sina intressen, kan det vara aktuellt att i stället skicka informationen till någon som kan ta tillvara hens intressen. Det kan till exempel gälla för barn och vissa personer med funktionsnedsättningar. I så fall bör i stället vårdnadshavare eller ställföreträdare få informationen för att kunna ta tillvara den registrerades dataskyddsrättsliga intressen.

När vi hämtar in uppgifter om en annan fysisk person än den försäkrade i ett förmånsärende enligt bestämmelserna i 110 kap. SFB, har vi sällan direktkontakt med personen i fråga. Vi behöver då utgå från att hen varken känner till eller förväntar sig att hens personuppgifter ska förekomma i våra behandlingar. Det innebär att hen inte, utan någon form av aktiv upplysning från vår sida, har anledning att leta upp och läsa den information som finns på vår webbplats om personuppgiftsbehandlingar. För att uppfylla kraven i artikel 14 behöver vi därför hitta lämpliga sätt att aktivt informera dessa personer om att vi har hämtat in uppgifter om dem.

11.3 Rätten till tillgång (registerutdrag)

En registrerad har rätt att få veta om vi behandlar hens personuppgifter. Hen har i så fall rätt att få tillgång till personuppgifterna, information om hur de används och om vissa rättigheter. I dataskyddsförordningen beskrivs rättigheten som ”rätten till tillgång”. Rättigheten brukar dock i Sverige kallas ”rätten till registerutdrag”.

Rätten till registerutdrag innebär även en rätt att få veta om vi *inte* behandlar personuppgifter. Om vi vid den aktuella tidpunkten inte behandlar några personuppgifter om den som begär registerutdraget ska vi lämna information om det. Det finns inte någon rätt att få veta om personuppgifter har behandlats tidigare.

Läs mer
Försäkringskassans riktlinjer (2008:11) *Hantering av information till den registrerade (registerutdrag)* beskriver hur du ska hantera en begäran om registerutdrag.

11.3.1 Innehållet i ett registerutdrag

Kopia av personuppgifter

Artikel 15.1 första stycket i dataskyddsförordningen
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 […]

Artikel 15.3 i dataskyddsförordningen
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.

Den registrerade har rätt att få en kopia av de personuppgifter som behandlas hos oss. Med ”kopia” avses de personuppgifter som en handling innehåller och inte handlingen i sig. Den registrerade kan dock ha rätt att få en kopia av utdrag ur handlingar eller till och med hela handlingar eller utdrag ur databaser om det är nödvändigt för att hen ska kunna utöva sina rättigheter enligt dataskyddsförordningen på ett effektivt sätt (jämför EU-domstolens dom Österreichische Datenschutzbehörde, C-487/21, EU:C:2023:369). Det kan exempelvis vara nödvändigt att lämna ut en kopia av en loggfil.

Rätten att få en kopia av de personuppgifter som behandlas gäller även uppgifter i handlingar som inte är allmänna (HFD 2025 not 30).

Vi är skyldiga att utnyttja alla de sök- och sammanställningsmöjligheter som vi har tillgång till på Försäkringskassan för att få fram personuppgifterna. Vi ska dock inte använda andra sökmöjligheter än de som är tillgängliga och tillåtna i vår verksamhet. Det finns inte något undantag från skyldigheten att lämna registerutdrag när det är omöjligt eller skulle innebära en oproportionell ansträngning att söka fram alla uppgifter om en person som behandlas (jämför undantaget i fråga om information när personuppgifter har samlats in från någon annan än den registrerade).

Vi bör göra sökningar i verksamhetsspecifika behandlingssystem, till exempel dokument- och ärendehanteringssystem, register och databaser. Även personuppgifter i rent administrativa register ska ingå i ett registerutdrag, till exempel register för lönehantering och inpassering. I den mån uppgifter är sökbara i standardprogram som Word, Outlook och Excel bör de också omfattas.

Det har inte ansetts rimligt att alla anställda i myndigheter med hundratals eller tusentals anställda var och en ska söka efter eventuella personuppgifter på egna lagringsytor vid varje förfrågan från en enskild (jämför prop. 2017/18:232 s. 231).

Informationen i kopian ska vara begriplig. Det innebär att förkortningar och liknande kan behöva förklaras. Det finns däremot inte någon skyldighet att förklara exempelvis medicinska eller tekniska termer. Inte heller finns det någon uttrycklig skyldighet att översätta uppgifterna om den registrerade inte förstår svenska (jämför Öman, *Dataskyddsförordningen [GDPR] m.m. En kommentar*, JUNO Version 4, kommentaren till artikel 12).

Det är som utgångspunkt endast personuppgifter om den registrerade själv som ska tas med i registerutdraget. Samtidigt kan en viss personuppgift vara personuppgift för flera olika fysiska personer. I första hand bör uppgifter om till exempel andra personer och företagshemligheter maskeras (göras oläsliga). Om det inte är möjligt att maskera uppgifter får det göras en intresseavvägning av om uppgifterna ska lämnas ut eller inte. För att kunna lämna ut personuppgifter om en annan registrerad i registerutdraget krävs att vi först prövar om det är förenligt med bland annat ändamålet med behandlingen av den andra personens personuppgifter. Även sekretess kan hindra att vi i ett registerutdrag lämnar ut uppgifter om någon annan fysisk person.

Rättsfall

Den registrerade begärde ett registerutdrag hos en kammarrätt som gällde handlingar som var föremål för sekretessprövning i ett mål om rätt att ta del av allmän handling där hen var klagande. Kammarrätten lämnade ut ett registerutdrag med sammanställningar av de personuppgifter som behandlades i de aktuella handlingarna. Kategorierna av personuppgifter som behandlades var hens namn, mejladress, personnummer och telefonnummer. HFD fann att dessa sammanställningar var tillräckliga för att den registrerade på ett effektivt sätt skulle kunna utöva sina rättigheter enligt dataskyddsförordningen. (HFD 2025 not 13)

Information om behandlingen

Artikel 15.1 och 2 i dataskyddsförordningen

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.

Den information som ska lämnas till den registrerade i registerutdraget ska som utgångspunkt lämnas på personuppgiftsnivå. För varje behandlad personuppgift ska vi alltså ange ändamålen med behandlingen, varifrån personuppgiften hämtats, till vilka personuppgiften lämnas ut och lagringstiden. (Öman, *Dataskyddsförordningen [GDPR] m.m. En kommentar*, JUNO Version 4, kommentaren till artikel 15)

Information om ändamålen ska vara specifik. Det räcker alltså inte att ange för vilka ändamål personuppgifterna kan behandlas, utan det ska framgå vilket eller vilka ändamål vi eftersträvar i det aktuella fallet. Om behandlingen utförs för flera olika ändamål måste den personuppgiftsansvariga klargöra vilka uppgifter eller vilka kategorier av uppgifter som behandlas för vilka ändamål (EDPB:s riktlinjer 01/2022 om registrerades rättigheter – rätt till tillgång, punkt 114).

Vem som ska anses vara mottagare definieras i artikel 4.9 i dataskyddsförordningen (se begreppslistan).

När vi har lämnat eller ska lämna ut personuppgifter är vi skyldiga att ge den registrerade den faktiska identiteten på mottagaren (EU-domstolens dom Österreichische Post, C-154/21, EU:C:2023:3, punkt 51). Det räcker alltså normalt sett

inte att endast lämna information om kategorier av mottagare. Undantag gäller om det är omöjligt att identifiera mottagarna eller vi kan visa att begäran om tillgång är uppenbart ogrundad eller orimlig.

Det finns som utgångspunkt inte någon rätt att få information om identiteten på anställda som har genomfört läsningar av den registrerades personuppgifter i enlighet med instruktioner från arbetsgivaren (jämför EU-domstolens dom Pankki S, C-579/21, EU:C:2023:501, punkt 83).

Enskilda som har begärt allmänna handlingar enligt TF ska inte anges som mottagare i registerutdrag. Försäkringskassan bör dock lämna information om att personuppgifter som finns i allmänna handlingar kan komma att lämnas ut enligt offentlighetsprincipen, om inte sekretess hindrar det.

Information om varifrån personuppgifter hämtas behöver inte sparas i syfte att ingå i registerutdrag. Vi bör inte behålla personuppgifter enbart för att kunna agera vid en potentiell begäran (skäl 64 till dataskyddsförordningen).

Om det förekommer automatiserat beslutsfattande, inbegripet profilering, ska vi lämna meningsfull information om detta i registerutdraget. Vad som avses med ”automatiserat beslutsfattande, inbegripet profilering” är inte klarlagt (se avsnitt 12.6).

Rättsfall
Den registrerade har rätt att få en förklaring av det förfarande och de principer som används vid automatiserat beslutsfattande, inbegripet profilering. Förklaringen ska vara av sådant slag att den registrerade kan förstå vilka av hens personuppgifter som har använts – och på vilket sätt – i samband med det automatiserade beslutsfattandet. Det räcker inte att åberopa att automatiserat beslutsfattande innefattar komplicerade processer. Det finns dock ingen skyldighet att lämna ut information om algoritmer som används inom ramen för automatiserat beslutsfattande. (EU-domstolens dom Dun & Bradstreet Austria, C-203/22, EU:C:2025:117)

11.3.2 Personuppgifter som inte ska ingå i ett registerutdrag

Undantag vid sekretess

Informationsskyldigheten omfattar inte sådana uppgifter som den enskilde inte får ta del av på grund av bestämmelser om sekretess (5 kap. 1 § dataskyddslagen). Det kan till exempel handla om uppgifter om den registrerades hälsotillstånd eller uppgifter om vem som har lämnat uppgifter om hen till Försäkringskassan (28 kap. 2 och 3 §§ OSL).

Det händer relativt sällan att uppgifter som ska ingå i ett registerutdrag är sekretessbelagda mot den registrerade själv, men en sekretessprövning måste ändå göras.

Undantag för löpande text som utgör utkast eller minnesanteckning

Rätten till registerutdrag omfattar inte personuppgifter i löpande text som inte har fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande (5 kap. 2 § dataskyddslagen). Det innebär att personuppgifter som finns i dokument som är under arbete eller som i övrigt är att betrakta som internt arbetsmaterial normalt sett inte ska ingå i ett registerutdrag (5 kap. 2 § första stycket dataskyddslagen). Personuppgifter i mejl omfattas ofta av detta undantag.

Undantaget gäller dock inte om personuppgifterna har lämnats ut till tredje part, behandlas enbart för arkivändamål av allmänt intresse eller statistiska ändamål, eller har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning (5 kap. 2 § andra stycket dataskyddslagen).

Andra skäl att utelämna uppgifter

Personuppgifter kan utelämnas från registerutdraget om den registrerade begär att det ska omfatta uppgifter som inte omfattas av skyldigheten att lämna registerutdrag eller för att begäran är uppenbart ogrundad eller orimlig (artikel 12.5 b i dataskyddsförordningen). Läs mer om när en begäran kan anses uppenbart ogrundad eller orimlig i avsnitt 11.3.5.

När uppgifter inte lämnas ut i ett registerutdrag, kan det ibland vara aktuellt att i stället hantera begäran som en begäran om partsinsyn eller om att få ta del av allmänna handlingar. Det beror på hur den registrerade har formulerat sin begäran. Det är i så fall viktigt att en sådan begäran tas om hand och omgående vidarebefordras till rätt funktion.

Tidigare begränsning i SFB gäller inte längre

Tidigare har det funnits en särskild bestämmelse i 114 kap. SFB med innebörden att personuppgifter i handlingar som kommit in i ett ärende eller upprättats i ett ärende inte behöver tas med i ett registerutdrag om den enskilde redan tagit del av handlingarnas innehåll. Den undantagsregeln gäller inte längre.

11.3.3 När ska vi lämna ett registerutdrag?

Ett registerutdrag förutsätter en begäran. Begäran ska som regel göras av den registrerade själv, även om hen är omyndig, har god man eller förvaltare. Men om hen själv inte kan tillgodogöra sig informationen i ett registerutdrag kan en vårdnadshavare, god man eller förvaltare begära registerutdraget (se Öman, *Dataskyddsförordningen [GDPR] m.m. En kommentar*, JUNO Version 4, kommentaren till artikel 4). Den registrerade kan också göra en begäran via ombud eller ställföreträdare (jämför EDPB:s riktlinjer om registrerades rättigheter – rätt till tillgång, punkt 80). Dödsbon kan inte begära registerutdrag (jämför prop. 2019/20:106 s. 32).

Det är möjligt att be den registrerade att lämna information som bekräftar hens identitet (artikel 12.6 i dataskyddsförordningen).

Det är ofta svårt för den registrerade att veta hur vi behandlar personuppgifter eller hur rätten till registerutdrag fungerar. En begäran kan därför vara formulerad på olika sätt. Den registrerade kan till exempel vilja ”få ut alla uppgifter som finns registrerade” om hen eller begära besked om hen ”förekommer i några avtal, handlingar eller register hos Försäkringskassan”. Om det är oklart vad den registrerade avser med sin begäran, bör vi ta kontakt med hen för att utreda vilken information hen vill ta del av.

Om vi behandlar en stor mängd uppgifter om den registrerade kan vi be hen precisera vilken information eller vilken behandling hen vill veta mer om, innan vi lämnar ut informationen (skäl 63 till dataskyddsförordningen och prop. 2023/24:29 s. 90). Vi har dock inte rätt att kräva att en begäran om registerutdrag begränsas.

Rätten till tillgång ska inte förväxlas med rätten till partsinsyn (insyn i det egna ärendet enligt 10 § FL, som omfattar material som har tillförts ärendet) eller rätten att ta del av allmän handling enligt bestämmelserna i TF. När uppgifter inte lämnas ut i ett registerutdrag, kan det ibland vara aktuellt att i stället hantera begäran som en begäran om partsinsyn eller en begäran om att få ta del av allmänna handlingar. Det förekommer också att en begäran omfattar både en begäran om registerutdrag och en begäran om

partsinsyn eller allmänna handlingar. Det är därför viktigt att fastställa vilka bestämmelser som en begäran grundar sig på.

Läs mer

Hur en begäran om att ta del av allmän handling ska hanteras framgår av Försäkringskassans riktlinjer (2011:7) *Utlämnande av allmänna handlingar och uppgifter*.

Hur en begäran om partsinsyn ska hanteras framgår av vägledningen (2004:7) *Förvaltningsrätt i praktiken*.

Utan onödigt dröjsmål

Vi ska hantera en begäran om registerutdrag utan onödigt dröjsmål och under alla omständigheter senast en månad efter att vi fått begäran (artikel 12.3 i dataskydds-förordningen). Inom denna tid ska vi alltså antingen ha tillmötesgått begäran eller meddelat att vi helt eller delvis inte kan göra det.

Tidsfristen får under vissa omständigheter förlängas och då ska vi lämna information om vad vi har gjort och varför vi inte kan hantera begäran inom en månad. Tiden kan förlängas med högst två månader.

11.3.4 Hur ska informationen i ett registerutdrag utformas?

Avsnitt 11.1.4 beskriver hur information till den registrerade ska utformas.

Om den registrerade gör en elektronisk begäran ska hen få informationen i ett elektroniskt format som är allmänt använt, om hen inte begär något annat (artikel 15.3 i dataskyddsförordningen). Detta gäller all information som den registrerade har rätt till enligt artikel 15.

Läs mer

Vad som gäller när personuppgifter skickas digitalt till externa mottagare framgår av Försäkringskassans anvisningar (2022:09) Säkerhet på Försäkringskassan.

11.3.5 Kostnad för registerutdrag

Ett registerutdrag är som regel kostnadsfritt. Men vi får ta ut en avgift om

- den registrerade återkommande begär registerutdrag på ett sådant sätt att en begäran kan anses uppenbart ogrundad eller orimlig (artikel 12.5 i dataskyddsförordningen)
- den registrerades begäran av annat skäl kan anses uppenbart ogrundad eller orimlig (artikel 12.5 i dataskyddsförordningen)
- den registrerade begär flera kopior på ett registerutdrag (artikel 15.3 i dataskyddsförordningen).

Om det blir aktuellt att ta ut avgift, gäller samma regler som för debitering vid begäran om att få ta del av allmän handling.

Rättsfall

EU-domstolen har uttalat att en begäran om att få tillgång till sina personuppgifter enligt artikel 15 i dataskyddsförordningen kan anses orimlig även om det är första gången som den registrerade gör en sådan begäran. Det kan vara fallet om det är möjligt att visa att den registrerade har haft en otillbörlig avsikt med begäran. Om det framgår av allmänt tillgängliga uppgifter att den registrerade har ägnat sig åt att begära ut sina personuppgifter från flera olika personuppgiftsansvariga och begära ersättning av dem, är detta en omständighet som kan läggas till grund för att anse att den registrerade haft en otillbörlig avsikt med den aktuella begäran. (EU-domstolens dom Brillen Rottler GmbH & Co. KG mot TC, C-526/24, EU:C:2026:216)

Läs mer

Vilka regler som gäller för debitering vid begäran om att få ta del av allmän handling framgår av Försäkringskassans riktlinjer (2011:7) *Utlämnande av allmänna handlingar och uppgifter*.

11.3.6 Avslagsbeslut

Om viss information i registerutdraget inte lämnas ut på grund av att den är sekretessbelagd gentemot den registrerade, ska hen alltid underrättas om möjligheten att få ett formellt avslagsbeslut. Vi ska fatta ett skriftligt beslut och skicka det till den registrerade om

- hen vill ha ett skriftligt beslut
- vi inte lämnar ut uppgifter av andra skäl, till exempel för att den registrerade begär att registerutdraget ska omfatta uppgifter som inte omfattas av skyldigheten att lämna registerutdrag eller för att begäran är uppenbart ogrundad eller orimlig.

I FL finns bland annat krav på dokumentation, kommunikation, utredningsskyldighet, motivering av beslut och överklagandehänvisning vid handläggning av ett ärende.

Läs mer

Läs mer om hur vi på Försäkringskassan hanterar ärenden enligt förvaltningsrättsliga bestämmelser i Försäkringskassans vägledning (2004:7) *Förvaltningsrätt i praktiken*.

Läs mer om avslagsbeslut vid begäran om registerutdrag i Försäkringskassans riktlinjer (2008:11) *Hantering av information till den registrerade (registerutdrag)*.

12 Övriga rättigheter

12.1 Rätten till rättelse

Artikel 16 i dataskyddsförordningen
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.

Vi kan göra en rättelse genom *ändring* eller genom *komplettering*. När den aktuella personuppgiften finns i en allmän handling ska rättelsen som huvudregel ske genom komplettering, oavsett om uppgiften är felaktig eller ofullständig med hänsyn till ändamålet med behandlingen (jämför HFD mål nr 5118-21 och KRNS mål nr 8588-21). Komplettering kan exempelvis göras genom att i anslutning till den felaktiga eller ofullständiga personuppgiften i it-systemet lägga till den korrekta personuppgiften. Att ta bort eller ändra en uppgift i en allmän handling kan nämligen innebära otillåten gallring.

Att en uppgift ger en felaktig bild av nuvarande förhållanden behöver inte betyda att uppgiften är felaktig i dataskyddsförordningens mening. Om det har funnits en avsikt eller en tanke bakom en registrering av en uppgift är utgångspunkten att den är riktig.

Uppgifter som en registrerad eller en annan myndighet har lämnat till Försäkringskassan anses exempelvis vara riktiga i dataskyddsförordningens mening om de registrerade uppgifterna stämmer överens med de uppgifter som faktiskt har lämnats. Detta gäller oavsett om de stämmer överens med de verkliga förhållandena eller inte. Om de registrerade uppgifterna är ofullständiga, med hänsyn till ändamålet med behandlingen, kan de ofta rättas genom komplettering.

I ett ärende hos Försäkringskassan är syftet med de personuppgifter som finns registrerade inte bara att visa dagsaktuella uppgifter, utan även att ge en bild av ärendets hela hantering. De olika personuppgifterna som har tillförts ett ärende över tid visar ett händelseförlopp, som behövs för att kunna handlägga ärendet. Uppgifterna anses därmed riktiga i dataskyddsförordningens mening.

Om vi tidigare har lämnat ut en personuppgift som senare rättas, kan vi vara skyldiga att informera mottagaren av personuppgiften om rättelsen. Vi behöver dock inte informera om det skulle visa sig vara omöjligt eller medföra en oproportionell ansträngning. Den registrerade har även rätt att begära att få information om vilka mottagare vi har lämnat personuppgifter till. (Artikel 19.2 i dataskyddsförordningen)

Vi har även en skyldighet att på eget initiativ rätta felaktiga personuppgifter. Det följer av de grundläggande principerna om uppgiftsminimering och korrekthet (artikel 5.1 c och d i dataskyddsförordningen, läs mer i avsnitt 3.3 och **Fel! Hittar inte referenskälla.**).

Rätten till rättelse gäller inte vid behandling av personuppgifter som är tillåten enligt lagen om den officiella statistiken eller enligt föreskrifter som har meddelats i anslutning till den lagen (15 a § lagen om den officiella statistiken).

Rätten till rättelse skiljer sig från bestämmelserna om rättelse eller ändring av beslut enligt 36–39 §§ FL.

Läs mer
Läs mer om vad som gäller vid rättelse enligt dataskyddsförordningen i Försäkringskassans riktlinjer (2008:25) *Registervård (rättelse, radering och begränsning enligt EU:s dataskyddsförordning)*.

Läs mer om rättelse och ändring av beslut enligt FL i Försäkringskassans vägledning (2018:1) *Rättelse och ändring av beslut enligt socialförsäkringsbalken och förvaltningslagen*.

12.2 Rätten till radering

Artikel 17 i dataskyddsförordningen
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.

Den registrerade har rätt att begära att få sina personuppgifter borttagna ur våra register på ett sådant sätt att de inte kan återskapas. Rätten till radering kallas även för rätten att bli bortglömd.

Om någon av punkterna i artikel 17.1 är uppfylld ska vi kontrollera om något undantag enligt artikel 17.3 är tillämpligt. Det räcker med att ett undantag är tillämpligt för att radering inte ska utföras. Det blir i praktiken mycket sällan bifall till en begäran om rätt till radering på en myndighet. Oftast gäller en eller flera undantagsbestämmelser för vår verksamhet.

Personuppgifterna som omfattas av en begäran av radering kan finnas både i en allmän handling och i material som inte utgör en allmän handling. Om personuppgifterna finns i allmänna handlingar saknas stöd för att radera dem om det inte finns något gallringsbeslut som är tillämpligt (läs mer om gallring i avsnitt 3.5).

Vi kan vara skyldiga att meddela mottagare som tidigare har tagit emot personuppgifter från oss om att vi har raderat någons personuppgifter. Vi behöver dock inte informera om det skulle visa sig vara omöjligt eller medföra en oproportionell ansträngning.

Läs mer

Läs mer om vad som gäller vid radering enligt dataskyddsförordningen i Försäkringskassans riktlinjer (2008:25) *Registervård (rättelse, radering och begränsning enligt EU:s dataskyddsförordning*).

12.3 Rätten till begränsning

Artikel 4.3 i dataskyddsförordningen
begränsning av behandling: markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden,

Artikel 18.1 i dataskyddsförordningen
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 riktighet, under en tid som ger den personuppgiftsansvarige möjlighet att kontrollera om personuppgifterna är riktiga.

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.

Att behandlingen begränsas innebär i praktiken att användningen av de aktuella personuppgifterna pausas tillfälligt eller avslutas permanent. Själva lagringen av personuppgifterna får dock fortsätta under tiden. Även viss behandling är tillåten (artikel 18.2 i dataskyddsförordningen).

En begränsning av personuppgiftsbehandling ställer krav på it-systemen. Det måste gå att på något sätt markera personuppgifterna som begränsade i systemet. Det måste också gå att tekniskt förhindra att uppgifterna fortsatt behandlas eller ändras under den tid som begränsningen gäller. Andra sätt för att begränsa behandlingen kan bland annat vara att de aktuella personuppgifterna tillfälligt flyttas till ett annat it-system, görs otillgängliga för användare eller tillfälligt tas bort från en webbplats (skäl 67 till dataskyddsförordningen).

Om vi har begränsat en behandling är vi skyldiga att meddela den registrerade innan vi upphör med begränsningen av behandlingen.

Vi kan vara skyldiga att meddela mottagare som tidigare tagit emot personuppgifter från oss om att vi har gjort en begränsning av någons personuppgifter (artikel 19 i

dataskyddsförordningen). Vi behöver inte informera om det skulle visa sig vara omöjligt eller medföra en oproportionell ansträngning.

Rätten till begränsning gäller inte vid behandling av personuppgifter som är tillåten enligt lagen om den officiella statistiken eller enligt föreskrifter som har meddelats i anslutning till den lagen (15 a § lagen om den officiella statistiken).

Rättsfall

Skatteverket hade avslagit en begäran om begränsning av personuppgifts-behandling endast med motiveringen att det inte kommit fram att kraven för begränsning enligt artikel 18 i dataskyddsförordningen var uppfyllda. Först under skriftväxling i domstol hade Skatteverket framfört att det inte fanns förutsättningar att begränsa behandlingen eftersom rätten till invändning inte gällde för den aktuella behandlingen. Kammarrätten bedömde att det endast är möjligt att neka en begärd begränsning enligt artikel 18.1 d i förordningen om det samtidigt motiveras varför det inte finns någon rätt till invändning enligt artikel 21. Skatteverket borde därför ha begränsat personuppgiftsbehandlingen tills de tagit ställning till rätten att invända mot behandlingen. (KRNS 7385-22)

Läs mer

Läs mer om vad som gäller vid begränsning enligt dataskyddsförordningen i Försäkringskassans riktlinjer (2008:25) *Registervård (rättelse, radering och begränsning enligt EU:s dataskyddsförordning)*.

12.4 Rätten till dataportabilitet

Den registrerade har enligt artikel 20 rätt till dataportabilitet. Det innebär en rätt att få ut sina personuppgifter i ett visst format och själv överföra dem till en annan personuppgiftsansvarig. Den registrerade har också rätt att på begäran få sina personuppgifter överförda direkt till en annan personuppgiftsansvarig när det är tekniskt möjligt.

Rätten till dataportabilitet gäller endast om personuppgiftsbehandlingen grundas på samtycke eller avtal och om behandlingen sker automatiserat. För Försäkringskassans del borde det därför vara ovanligt att rätten aktualiseras. Det skulle kunna vara aktuellt när anställdas personuppgifter behandlas endast med stöd av avtal eller samtycke som rättslig grund.

12.5 Rätten att göra invändningar

Artikel 21.1 i dataskyddsförordningen

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.

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.

Den registrerade har rätt att göra invändningar mot behandling av hens personuppgifter när behandlingen sker för att utföra en uppgift av allmänt intresse eller som ett led i vår myndighetsutövning (artikel 6.1 e i dataskyddsförordningen) alternativt efter en intresseavvägning (artikel 6.1 f i dataskyddsförordningen). Det innebär att den registrerade inte kan invända mot behandling som grundas på ett avtal, till exempel ett anställningsavtal.

En majoritet av Försäkringskassans personuppgiftsbehandlingar sker med stöd av artikel 6.1 e (se avsnitt 4.2.4). Rätten att göra invändningar gäller dock inte när vi behandlar personuppgifter inom kärnverksamheten (114 kap. 6 § SFB). Inte heller gäller rätten att göra invändningar vid behandling av personuppgifter som omfattas av lagen om den officiella statistiken (prop. 2017/18:107 s. 30 f.). I praktiken finns det därmed inte så många behandlingar hos Försäkringskassan som den registrerade kan invända mot.

12.6 Rätten att slippa automatiserat beslutsfattande, inbegripet profilering

Artikel 4.4 i dataskyddsförordningen

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,

Artikel 22.1 i dataskyddsförordningen

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.

Vad som menas med ”beslut som enbart grundas på automatiserad behandling, inbegripet profilering” är inte klarlagt. Enligt IMY och EDPB omfattar skrivningen både automatiserade beslut som grundas på profilering och automatiserade beslut som inte

grundas på profilering. Regeringen har dock bedömt att avsikten med artikel 22 har varit att endast omfatta automatiserade beslut som innefattar profilering men noterar att någon säker slutsats inte kan dras i denna fråga i avsaknad av praxis (prop. 2017/18:95 s. 100).

I den juridiska litteraturen anser flera författare att artikel 22 borde tolkas på ett sådant sätt att enbart automatiserade beslut som grundas på profilering omfattas (se Öman, *Dataskyddsförordningen [GDPR] m.m. En kommentar*, JUNO Version 4, kommentaren till artikel 22 och Westman, *Karnovs lagkommentar 232 till artikel 22 i dataskyddsförordningen*, JUNO Version 2026-07-01).

Förbudet mot automatiserat beslutsfattande, inbegripet profilering, gäller inte under vissa förutsättningar (artikel 22.2 i dataskyddsförordningen). Det är bland annat möjligt att göra undantag från förbudet i nationell rätt. Ett sådant undantag har gjorts i 28 § FL, som ger myndigheter en generell rätt att fatta automatiserade beslut, däribland automatiserade beslut som grundas på profilering. Regeringen anser att kravet på lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen är tillgodosett genom den förvaltningsrättsliga regleringen (se prop. 2017/18:95 s. 100).

Automatiserade beslut, inbegripet profilering, får grundas på känsliga personuppgifter endast om behandlingen grundas på samtycke (artikel 9.2 a i dataskyddsförordningen) eller är nödvändig av hänsyn till ett viktigt allmänt intresse på grundval av unionsrätten eller svensk rätt (artikel 9.2 g i dataskyddsförordningen). Lämpliga åtgärder som skyddar den registrerades berättigade intressen ska då ha vidtagits (artikel 22.4 i dataskyddsförordningen). För behandling av känsliga personuppgifter i vår kärnverksamhet gäller 114 kap. 11 § SFB (avsnitt 6.6.1).

Som framgår av avsnitt 4.2.1 är det ovanligt att en personuppgiftsbehandling som utförs av en myndighet grundas på samtycke.

Rekvisiten i artikeln

Med rekvisitet ”beslut som enbart grundar sig på automatiserad behandling” menas att beslutsprocessen är helt automatiserad och utan mänsklig inblandning. För att ett beslut ska anses ha mänsklig inblandning krävs att en människa granskar det och att granskningen sker på ett meningsfullt sätt snarare än enbart som en symbolisk gest. Den person som granskar behöver också ha behörighet och kompetens att ändra beslutet. (Artikel 29-gruppens riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning [EU] 2016/679 (WP 251 rev.01), s. 21 f.)

Artikel 29-gruppen beskriver profilering på bland annat följande sätt:

> ”I huvudsak innebär profilering att man samlar in information om en person (eller en grupp personer) och bedömer deras personliga egenskaper eller beteendemönster för att placera in dem i en viss kategori eller grupp, särskilt för att analysera och/eller göra förutsägelser om till exempel deras förmåga att utföra en uppgift, intressen, eller sannolikt beteende.” (Artikel 29-gruppens riktlinjer om automatiserat individuellt beslutsfattande och profilering s. 7 f.)

Bestämmelsen gäller inte för beslut som delvis fattas automatiserat, till exempel när resultatet från automatiserad behandling baserad på profilering används för att ge stöd för mänskligt beslutsfattande.

Beslut med *rättsliga följder* är till exempel beslut som beviljar eller avslår en ansökan om en särskild lagstadgad social förmån. Beslut som påverkar en persons finansiella situation eller ger hen en stor nackdel är exempel på vad som ”på liknande sätt i

betydande grad påverkar honom eller henne”. (Artikel 29-gruppens riktlinjer om automatiserat individuellt beslutsfattande och profilering, s. 22)

Förbudet mot beslut som enbart grundas på automatiserad behandling, inbegripet profilering, gäller utan att den registrerade behöver göra en begäran (se EU-domstolens dom SCHUFA Holding [Profilering], C-634/21, EU:C:2023:957, punkt 52).

Rättsfall

Ett kreditupplysningsföretag fastställde ett sannolikhetsvärde gällande framtida återbetalningsförmåga grundat på personuppgifter om en fysisk person genom automatiserad behandling. Detta sannolikhetsvärde överfördes till en tredje part, och den tredje parten lade i avgörande grad detta värde till grund för sitt beslut om att ingå, fortsätta eller avsluta ett avtalsförhållande med den fysiska personen. EU-domstolen bedömde att förfaringssättet grundade sig på en automatiserad behandling som hade följder som i betydande grad påverkade den registrerade. (EU-domstolens dom SCHUFA Holding [Profilering], C-634/21, EU:C:2023:957).

Läs mer

Läs mer om artikel 22 och automatiserat beslutsfattande i vägledningen (2024:3) Digitalisering på Försäkringskassan.

12.7 Kostnad och beslut

Som huvudregel ska det vara kostnadsfritt för den registrerade att utöva sina rättigheter enligt dataskyddsförordningen. Om en begäran från en registrerad enligt artiklarna 16–21 är uppenbart ogrundad eller orimlig, särskilt på grund av dess repetitiva art, får den personuppgiftsansvariga antingen ta ut en rimlig avgift som täcker de administrativa kostnaderna för att tillhandahålla den information eller vidta den åtgärd som begärts, eller vägra att tillmötesgå begäran (artikel 12.5 i dataskyddsförordningen). Läs mer om när en begäran kan anses uppenbart ogrundad eller orimlig i avsnitt 11.3.5.

Om vi inte tillmötesgår en enskilds begäran enligt artiklarna 16–21, ska den enskilde få ett formellt avslagsbeslut. I FL finns bland annat krav på dokumentation, kommunikation, utredningsskyldighet, motivering av beslut och överklagandehänvisning vid handläggning av ett ärende.

Läs mer

Läs mer om hur vi på Försäkringskassan hanterar ärenden enligt förvaltningsrättsliga bestämmelser i Försäkringskassans vägledning (2004:7) *Förvaltningsrätt i praktiken*.

13 Konsekvensbedömning

Artikel 35.1 i dataskyddsförordningen
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.

En konsekvensbedömning är en pågående process för att identifiera, bedöma och hantera de risker som vissa personuppgiftsbehandlingar medför. Att det är en pågående process innebär att det inte är en arbetsuppgift som utförs vid ett enskilt tillfälle för att sedan kunna markeras som klar. Så länge vi utför personuppgiftsbehandlingen, ska konsekvensbedömningen därför vara levande.

13.1 Vad ska vi bedöma?

Det som ska bedömas är *typen av personuppgiftsbehandling.* Det första steget är därför att ringa in och identifiera personuppgiftsbehandlingen. Definitionen av vad som är en behandling finns i artikel 4.2 i dataskyddsförordningen: ”en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter […]”.

Att bedöma typen av behandling innebär att bedöma behovet av en konsekvensbedömning som om inga riskreducerande eller riskeliminerande åtgärder har vidtagits för att göra behandlingen säkrare (IMY, *Vägledning vid konsekvensbedömning, Rättsligt tolkningsstöd*, februari 2025, s. 13).

När vi ska bedöma behovet av konsekvensbedömningar för personuppgiftsbehandlingar som redan pågår hos oss, måste vi alltså bortse från de åtgärder som vi redan har vidtagit. Vi redogör sedan för åtgärderna i de eventuella konsekvensbedömningarna.

En konsekvensbedömning kan också omfatta flera behandlingar om de liknar varandra. Det kan vara onödigt att upprätta en helt ny konsekvensbedömning om en liknande behandling redan har analyserats och bedömts. För att behandlingar ska kunna omfattas av en och samma konsekvensbedömning krävs det dock att de liknar varandra när det gäller art, omfattning, sammanhang, ändamål och risker (Artikel 29-gruppens 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, s. 8). Enligt IMY krävs det att behandlingarna är mycket lika varandra för att de ska kunna omfattas av en och samma konsekvensbedömning (IMY, Rättsligt tolkningsstöd, s. 25).

Läs mer
Läs mer om hur vi på Försäkringskassan avgränsar våra personuppgifts-behandlingar i Försäkringskassans riktlinjer (2024:03) *Bedöma och dokumentera personuppgiftsbehandlingar*.

13.2 När ska vi göra en konsekvensbedömning?

En konsekvensbedömning ska göras för behandlingar som sannolikt innebär en hög risk för fysiska personers rättigheter och friheter. För att avgöra om en behandling sannolikt innebär en hög risk behöver vi göra en initial bedömning. På Försäkringskassan kallas den initiala bedömningen för grundläggande bedömning.

När vi bedömer om risken med en behandling sannolikt är hög ska vissa faktorer beaktas (artikel 35.1 i dataskyddsförordningen).

Ny teknik

Användningen av ny teknik ska särskilt beaktas. Det beror på att konsekvenserna ofta kan vara okända när ny teknik används. Vad som räknas som ”ny teknik” är av förklarliga skäl något som regelbundet behöver utvärderas eftersom det beror på den senaste utvecklingen och den senaste tekniska kunskapen. Det vara till exempel vara fråga om artificiell intelligens, maskininlärning eller djupinlärning (IMY, *Rättsligt tolkningsstöd,* s. 13). Även ”gammal” teknik som används på nya sätt kan tala för att en konsekvensbedömning behöver göras (Artikel 29-gruppens riktlinjer om konsekvensbedömning, s. 10).

Art

Behandlingens art tar sikte på vilken typ av behandling det rör sig om, hur vi kommer att utföra den, vad det ingår för slags personuppgifter och vilka kategorier av registrerade som uppgifterna tillhör (IMY, *Rättsligt tolkningsstöd,* s. 14). Faktorer i form av behandling av känsliga personuppgifter, att sårbara individer ingår som registrerade eller att behandlingen utförs på integritetskränkande sätt talar för att risken med behandlingen ska bedömas högre.

Omfattning

Behandlingens omfattning innebär att vi behöver beakta volymen av personuppgifter som behandlas och antalet registrerade som ingår. Vi behöver också beakta hur länge behandlingen ska pågå, hur ofta den ska utföras och dess geografiska omfattning (IMY, *Rättsligt tolkningsstöd,* s. 14).

Sammanhang

Med behandlingens sammanhang menas att vi ska se behandlingen i ett större perspektiv. Vi behöver beakta var uppgifterna kommer ifrån, vår relation till de enskilda och i vilken utsträckning som de registrerade har kontroll över sina personuppgifter. Vi behöver också beakta om behandlingen är något som de registrerade kan förvänta sig eller om den kan uppfattas som oförutsägbar.

Ändamål

Med behandlingens ändamål menas anledningen till varför vi vill genomföra behandlingen. Vissa ändamål anses mer integritetskänsliga än andra. Behandlingar som till exempel innebär övervakning, kontroll, att vissa personer pekas ut eller profileras bör anses som känsligare och därmed innebära en högre risk.

Artikel 35.3 i dataskyddsförordningen
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.

I artikel 35.3 finns exempel på typer av personuppgiftsbehandlingar som särskilt kräver att det görs konsekvensbedömningar.

Led a

En konsekvensbedömning ska göras om behandlingen innebär en omfattande och systematisk bedömning av fysiska personers personliga aspekter. Bedömningen behöver också grunda sig på en automatisk behandling, inbegripet profilering. Beslutet behöver leda till rättsliga följder eller på liknande sätt och i betydande grad påverka fysiska personer. Beslutet behöver inte enbart grundas på automatisk behandling, inbegripet profilering, för att behandlingen ska omfattas av led a (se Öman, *Dataskyddsförordningen [GDPR] m.m. En kommentar*, JUNO Version 4, kommentaren till artikel 35).

Led b

En konsekvensbedömning behöver särskilt göras vid behandling i stor omfattning av känsliga personuppgifter eller av personuppgifter om lagöverträdelser.

Det finns ingen exakt definition eller uttalade värden som anger vad ”stor omfattning” är, utan bedömningen får göras från fall till fall. I bedömningen rekommenderar EDPB (Artikel 29-gruppens riktlinjer om dataskyddsombud s. 8) att man tar hänsyn till:

- Antalet registrerade, antingen det exakta antalet eller som en andel av den aktuella populationen.
- Mängden personuppgifter och/eller de olika kategorier av personuppgifter som behandlas.
- Under hur lång tid som behandlingen pågår.
- Behandlingens geografiska räckvidd.

Led c

Enligt detta led ska en konsekvensbedömning särskilt göras om typen av behandling innebär en systematisk övervakning av allmän plats i stor omfattning. Med *systematisk* övervakning menas att övervakningen till exempel sker enligt ett system, är organiserad eller metodisk eller utförs som en del av en strategi (Artikel 29-gruppens riktlinjer om konsekvensbedömning, s. 10). Allmän plats innebär platser dit allmänheten har tillträde, till exempel gator, torg och bibliotek (Artikel 29-gruppen riktlinjer om konsekvens-bedömning, s. 11).

13.2.1 IMY:s förteckning

Artikel 35.4 i dataskyddsförordningen
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.

I enlighet med artikel 35.4 har IMY tagit fram en förteckning med nio kriterier för behandlingar som sannolikt medför en hög risk och som innebär att en konsekvensbedömning behöver göras. En behandling medför sannolikt en hög risk om den innebär

- utvärdering eller poängsättning av människor (till exempel genetiska tester till konsumenter för att bedöma och förutse risker för sjukdomar, och profilering av internetanvändare)
- behandling av personuppgifter i syfte att fatta automatiserade beslut som har rättsliga följder eller liknande betydande följder för den registrerade
- systematisk övervakning av människor (till exempel kameraövervakning av en allmän plats och insamling av personuppgifter från internetanvändning i offentliga miljöer)
- behandling av känsliga personuppgifter enligt artikel 9.2 eller uppgifter som är av mycket personlig karaktär (till exempel vårdens lagring av patientjournaler, insamling av lokaliseringsuppgifter och bankers hantering av finansiella uppgifter)
- behandling av personuppgifter i stor omfattning
- kombination av personuppgifter från två eller flera behandlingar på ett sätt som avviker från vad de registrerade rimligen kunnat förvänta sig (till exempel samkörning av register)
- behandling av personuppgifter som avser personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara (till exempel barn, anställda, asylsökande, äldre och patienter)
- användning av ny teknik eller nya organisatoriska lösningar (till exempel en sakernas internet-applikation ([Internet of things, IoT])
- behandling av personuppgifter i syfte att hindra registrerade från att få tillgång till en tjänst eller ingå ett avtal (till exempel en banks granskning av sina kunder mot en databas för kreditupplysning för att besluta om de ska erbjudas lån).

Som huvudregel behöver minst två av kriterierna vara uppfyllda för att behandlingen ska träffas av kravet på att genomföra en konsekvensbedömning.

Utöver listan med kriterier innehåller IMY:s förteckning också exempel på behandlingar för vilka IMY rekommenderar att en konsekvensbedömning genomförs, till exempel övervakning av anställdas användning av internet och mejl samt myndigheter som genom digitala plattformar ger service till befolkningen. I förteckningen anges också att en behandling skulle kunna uppfylla två kriterier men ändå inte anses sannolikt leda till en hög risk. I de fallen måste vi dokumentera och motivera vår bedömning, samt inhämta dataskyddsombudets synpunkter (IMY, Förteckning enligt artikel 35.4 i dataskyddsförordningen, 2019-01-16, DI-2018-13200).

Läs mer
Dataskyddsombudets roll vid genomförande av konsekvensbedömningar finns beskriven i Försäkringskassans riktlinjer (2024:03) Bedöma och dokumentera personuppgiftsbehandlingar och anvisningarna (2025:19) Bedöma och dokumentera personuppgiftsbehandlingar.

13.3 Vad en konsekvensbedömning ska innehålla

Enligt artikel 35.7 i dataskyddsförordningen ska en konsekvensbedömning åtminstone innehålla:

- en systematisk beskrivning av behandlingen och dess syften
- en bedömning av behandlingens behov och av behandlingens proportionalitet i förhållande till syftena
- en bedömning av riskerna för registrerades fri- och rättigheter
- en beskrivning av de åtgärder som vidtas för att minimera riskerna.

Bestämmelsen i artikel 35.7 ger uttryck för minimikraven för innehållet i en konsekvensbedömning. Hur kraven ska tolkas framgår i flera olika riktlinjer och vägledningar från olika aktörer, till exempel olika tillsynsmyndigheter och EU-organ. Enligt bland annat Artikel 29-gruppen och IMY innehåller varje krav flera delar som behövs för att den sammantagna bedömningen ska anses tillräcklig. IMY rekommenderar till exempel att den systematiska beskrivningen av behandlingen omfattar behandlingens art, omfattningen, sammanhang, ändamål, nödvändiga resurser, en funktionell beskrivning av behandlingen samt roller och ansvarsfördelning. Behandlingens art bör sedan i sin tur bestå av en allmän beskrivning och bakgrund samt en beskrivning av kategorier av personuppgifter och kategorier av registrerade.

Läs mer
Läs mer om innehållet i en konsekvensbedömning i Artikel 29-gruppens 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) (särskilt bilaga 2).

Läs också mer i IMY:s *Vägledning vid konsekvensbedömning, En praktisk guide,* februari 2025.

13.4 Inhämtande av synpunkter från registrerade

Artikel 35.9 i dataskyddsförordningen
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.

I samband med att en konsekvensbedömning genomförs ska den personuppgiftsansvariga hämta in synpunkter från de aktuella registrerade eller deras företrädare om den avsedda behandlingen, om det bedöms vara lämpligt. Det kan till

exempel vara lämpligt att inhämta synpunkter från fackförbund eller intresseorganisationer.

13.5 Undantag från kravet att göra en konsekvensbedömning

Om en behandling grundar sig på en rättslig förpliktelse (artikel 6.1 c), ett allmänt intresse eller utförs som ett led i myndighetsutövning (artikel 6.1 e) innebär det att grunden för behandlingen regleras i en bestämmelse som finns i unionsrätten eller i vår nationella rätt (se avsnitt 4.2.3 och 4.2.4). I samband med lagstiftningsprocessen för dessa bestämmelser finns det möjlighet för lagstiftaren att göra en konsekvensbedömning, som en del av en allmän konsekvensbedömning, för de personuppgiftsbehandlingar som följer av bestämmelserna. (Artikel 35.10 i dataskyddsförordningen)

I de fall då vår behandling grundar sig på rättslig förpliktelse, allmänt intresse eller myndighetsutövning och lagstiftaren redan har gjort en konsekvensbedömning behöver vi alltså inte bedöma behandlingen, trots att behandlingen sannolikt leder till en hög risk för fysiska personers fri- och rättigheter.

13.6 Förhandssamråd

Artikel 36.1 i dataskyddsförordningen

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 personuppgifts-ansvarige vidtar åtgärder för att minska risken.

Om en konsekvensbedömning visar att det finns kvarstående höga risker även efter våra planerade åtgärder behöver vi begära förhandssamråd med IMY om vi vill gå vidare med behandlingen. För att kunna begära förhandssamråd behöver det finnas en gedigen och väl dokumenterad konsekvensbedömning. IMY har en blankett för att begära förhandssamråd på deras webbplats (www.imy.se).

Om IMY anser att behandlingen strider mot dataskyddsförordningen har IMY åtta veckor på sig att besvara begäran. Om den planerade behandlingen är komplicerad får denna tid förlängas med sex veckor. Svaret från IMY ska innehålla skriftliga råd. IMY får i samband med hanteringen av begäran också utnyttja de befogenheter som de har enligt artikel 58, till exempel beordra att de ges tillgång till ytterligare information och tillgång till personuppgifter. Om IMY inte besvarar en begäran så får vi påbörja behandlingen. Ett uteblivet svar hindrar dock inte IMY från att vid ett senare tillfälle ingripa mot behandlingen (skäl 94 till dataskyddsförordningen).

Rättsfall

Enligt kammarrätten i Stockholm hade Gymnasienämnden i Skellefteå kommun inte gjort en tillräckligt noggrann riskbedömning när de införde närvarokontroll genom ansiktsigenkänning på en gymnasieskola. Behandlingen var av sådan art att förhandssamråd borde ha begärts (KRNS mål nr 5888-20).

14 Register över personuppgiftsbehandlingar

Artikel 30.1 i dataskyddsförordningen
Varje personuppgiftsansvarig och, i tillämpliga fall, dennes företrädare ska föra ett register över behandlingar som utförts under dess ansvar. […]

Artikel 30.2 i dataskyddsförordningen
Varje personuppgiftsbiträde och, i tillämpliga fall, dennes företrädare ska föra ett register över alla kategorier av behandling som utförts för den personuppgiftsansvariges räkning, […]

Försäkringskassan är i egenskap av personuppgiftsansvarig skyldig att föra ett register över våra personuppgiftsbehandlingar. Vi är också skyldiga att föra register över de behandlingar som vi utför åt andra i egenskap av personuppgiftsbiträde. Registren ska föras i skriftlig form och göras tillgängliga för IMY om de skulle begära det (artikel 30.3 och 30.4 i dataskyddsförordningen).

Registren är också ett sätt för Försäkringskassan att uppfylla ansvarsskyldigheten enligt artikel 5.2 (läs mer i avsnitt 3.7), eftersom de ger oss kontroll och överblick över våra behandlingar.

14.1 Register över personuppgiftsbehandlingar i egenskap av personuppgiftsansvarig

Registret över våra personuppgiftsbehandlingar i egenskap av personuppgiftsansvarig ska innehålla följande uppgifter:

- Namn och kontaktuppgifter för Försäkringskassan.
- Namn och kontaktuppgifter till den eller de som vi eventuellt är gemensamt personuppgiftsansvarig med.
- Namn och kontaktuppgifter till eventuella företrädare för Försäkringskassan.
- Namn och kontaktuppgifter för dataskyddsombudet.
- Ändamål med behandlingen.
- Vilka kategorier av registrerade och vilka kategorier av personuppgifter som ingår i behandlingen.
- De kategorier av mottagare som personuppgifterna har lämnats ut eller ska lämnas ut till. Detta gäller även för mottagare i tredjeländer eller i internationella organisationer.
- Information om eventuella överföringar till tredjeland eller en internationell organisation. Det ska då anges vart uppgifter överförs, alltså till vilket land eller organisation. Om överföringen sker med stöd av ett av undantagen i artikel 49.1 i dataskyddsförordningen ska det anges vilka lämpliga skyddsåtgärder som vidtas.
- Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.
- Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1 i dataskyddsförordningen.

14.2 Register över personuppgiftsbehandlingar i egenskap av personuppgiftsbiträde

Registret över de behandlingar som vi utför i egenskap av personuppgiftsbiträde ska innehålla följande uppgifter:

- Namn och kontaktuppgifter för Försäkringskassan.
- Namn och kontaktuppgifter för eventuella företrädare som vi eller den personuppgiftsansvariga har.
- Namn och kontaktuppgifter till varje personuppgiftsansvarig för vars räkning vi behandlar personuppgifter.
- Namn och kontaktuppgifter till dataskyddsombudet.
- Den typ av behandling som utförs för varje personuppgiftsansvarigs räkning. Till exempel strukturering, lagring eller bearbetning.
- Information om eventuella överföringar till tredjeland eller en internationell organisation. Det ska då anges var uppgifter överförs, alltså till vilket land eller organisation. Om överföringen sker med stöd av ett av undantagen i artikel 49.1 ska det anges vilka lämpliga skyddsåtgärder som vidtas.
- Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1 i dataskyddsförordningen.

Läs mer

I Försäkringskassans riktlinjer (2024:3) *Bedöma och dokumentera personuppgiftsbehandlingar* och i anvisningarna (2025:19) *Bedöma och dokumentera personuppgiftsbehandlingar* kan du läsa mer om hur vi på Försäkringskassan har fördelat ansvaret för registren och hur behandlingar anmäls in och dokumenteras.

15 Personuppgiftsincidenter

Artikel 4.12 i dataskyddsförordningen
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,

I skäl 85 till dataskyddsförordningen står det att en personuppgiftsincident som inte snabbt åtgärdas på lämpligt sätt kan leda till fysisk, materiell eller immateriell skada för fysiska personer. Den kan också leda till bland annat diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, skadat anseende, sekretessbrott eller till annan ekonomisk eller social nackdel för den berörda fysiska personen. Felskickade mejl, borttappade mobiltelefoner eller att handläggare råkar lägga in personuppgifter i fel ärende är exempel på händelser som kan utgöra personuppgiftsincidenter.

15.1 När ska vi anmäla en personuppgiftsincident till IMY?

Vi ska anmäla en personuppgiftsincident till IMY om det inte är osannolikt att den medför en risk för fysiska personers rättigheter och friheter. Vi ska göra det utan onödigt dröjsmål, men inte senare än 72 timmar efter att vi har fått vetskap om incidenten. Om vi gör anmälan efter 72 timmar ska vi motivera förseningen (artikel 33.1 i dataskydds-förordningen).

Vi anses ha fått vetskap om incidenten när vi kan vara rimligt säkra på att en personuppgiftsincident har inträffat och att personuppgifter har äventyrats (EDPB:s riktlinjer 9/2022 om anmälan av personuppgiftsincidenter enligt den allmänna dataskyddsförordningen, s. 11). När en personuppgiftsansvarig anses vara ”rimligt säker” beror på omständigheterna i det enskilda fallet. För vissa incidenter kan det redan i ett tidigt skede stå klart att incidenten involverar personuppgifter och att skyddet för dem har riskerats. Andra incidenter kan kräva att vi utreder omständigheterna mer noggrant innan vi kan konstatera att det som skett utgör en personuppgiftsincident. När vi har konstaterat att det rör sig om en personuppgiftsincident börjar de 72 timmarna att löpa.

Ett personuppgiftsbiträde som får vetskap om en personuppgiftsincident ska informera oss utan onödigt dröjsmål (artikel 33.2 i dataskyddsförordningen).

I vissa fall är det inte möjligt för oss att få fram all relevant information om personuppgiftsincidenten, innan anmälan ska skickas in. Då kan vi lämna informationen till IMY i omgångar och alltså komplettera anmälan i efterhand (artikel 33.4 i dataskydds-förordningen).

Läs mer
Medarbetare anmäler potentiella personuppgiftsincidenter via Min Support. Hur hanteringen av incidenter går till framgår av Försäkringskassans anvisningar (2022:07) *Hantering av säkerhetsincidenter* där avsnitt 3.3.1 särskilt tar upp personuppgiftsincidenter.

15.1.1 Bedöma risken vid en incident

När vi bedömer risken för fysiska personers friheter och rättigheter vid en inträffad personuppgiftsincident bör vi ta hänsyn till

- hur *sannolikt* det är att risken leder till skada
- riskens *svårighetsgrad*, alltså hur allvarlig skadan kan tänkas vara

(skäl 75 och 76 till dataskyddsförordningen).

Om vi inte är säkra på hur hög risken ska anses vara bör vi ta det säkra före det osäkra och anmäla den till IMY (EDPB:s riktlinjer om anmälan av personuppgiftsincidenter enligt den allmänna dataskyddsförordningen, s. 27). Utredningen görs av en säkerhetsrådgivare som har rollen som incidentutredare i processen för incidenthantering (anvisningarna [2022:07] *Hantering av säkerhetsincidenter*). Om risken bedöms som hög ska vi informera de registrerade. Läs mer om information till de registrerade i avsnitt 15.2.

När vi bedömer risken vid en personuppgiftsincident rekommenderar EDPB (riktlinjer om anmälan av personuppgiftsincidenter enligt den allmänna dataskyddsförordningen, s. 24 ff.) att vi bland annat tar hänsyn till följande:

- **Vad det är för typ av incident.** Om den till exempel innebär att personuppgifter har röjts för obehöriga eller att uppgifter har ändrats och inte längre är korrekta. Den kan också medföra brist på tillgänglighet till exempel på grund av ett driftstopp. Om incidenten orsakats avsiktligt med ont uppsåt, till exempel på grund av ett antagonistiskt angrepp, bör detta påverka bedömningen av risken.
- **Kategorier av personuppgifter och volym.** Ju känsligare personuppgifter som omfattas av incidenten, desto högre bör risken anses vara. Om flera olika kategorier av personuppgifter ingår och kan kombineras påverkar även detta bedömningen. En stor mängd detaljer kan avslöja ännu mer information om just den personen. En incident som påverkar stora volymer personuppgifter om många registrerade kan få effekter för ett motsvarande stort antal enskilda personer.
- **Hur enkelt det är att identifiera enskilda.** Om incidenten innebär att personuppgifter har röjts för obehöriga och det är enkelt för dem att identifiera enskilda bör detta innebära att risken bedöms som högre. Här bör vi även beakta om uppgifterna kan kombineras med allmänt tillgänglig information som förenklar identifiering.
- **Kategorier av registrerade och hur många som påverkas.** Om incidenten omfattar individer som är sårbara, till exempel barn, kan det innebära att risken ska bedömas som högre.
- **Vad incidenten kan få för konsekvenser för enskilda och hur allvarliga de är.** Konsekvenserna för enskilda vid en incident som bedöms vara särskilt svåra är bedrägeri, identitetsstöld, ekonomisk förlust, skadat anseende, psykisk oro, stress, irritation, tidsförlust med mera. Att personuppgifterna röjs för en betrodd mottagare, exempelvis en annan avdelning inom samma verksamhet, som agerar snabbt för att begränsa skadan genom att till exempel skicka tillbaka uppgifterna skulle kunna vara en faktor som talar mot allvarliga konsekvenser för de registrerade.

Läs mer
ENISA (European Union Agency for Network and Information Security, EU:s cybersäkerhetsbyrå) har tillsammans med tillsynsmyndigheter i Grekland och Tyskland tagit fram en metodik som de rekommenderar att personuppgifts-ansvariga använder sig av vid bedömning av personuppgiftsincidenter. Se *Recommendations for a methodology of the assessment of severity of personal data breaches*, Working Document, v1.0, December 2013.

15.1.2 Undantag från att anmäla en incident till IMY

Om riskbedömningen visar att det är *osannolikt* att en inträffad personuppgiftsincident medför en risk för fysiska personers rättigheter och friheter behöver vi inte anmäla den till IMY. Till exempel bör vi inte anmäla incidenter om felskickad post eller mejl som varken innehåller känsliga personuppgifter eller andra personuppgifter som kan användas på ett skadligt sätt. EDPB rekommenderar dock att den personuppgifts-ansvariga vidtar vissa åtgärder, till exempel identifierar hur felet kunde inträffa, inför ytterligare kontrollmekanismer och ber den icke avsedda mottagaren av posten eller mejlet att förstöra eller radera det felskickade underlaget (EDPB:s riktlinjer 01/2021 om exempel på anmälan av personuppgiftsincidenter, s. 28 ff.).

Även om vi inte behöver anmäla en personuppgiftsincident till IMY, måste vi dokumentera den internt. Dokumentationen ska innehålla

- en beskrivning av omständigheterna kring incidenten,
- vilka effekter den har fått
- vilka åtgärder som har vidtagits

(artikel 33.5 i dataskyddsförordningen).

EDPB rekommenderar också att personuppgiftsansvariga dokumenterar sin bedömning av risken och motiverar varför den inte behövde anmälas till tillsynsmyndigheten (EDPB:s riktlinjer om exempel på anmälan av personuppgiftsincidenter, s. 28).

15.2 När ska vi informera de registrerade?

Om en personuppgiftsincident sannolikt leder till en *hög* risk för fysiska personers rättigheter och friheter ska vi enligt artikel 34 i dataskyddsförordningen utan onödigt dröjsmål informera de registrerade om incidenten. Enligt EDPB ska risken anses som hög om incidenten kan medföra fysiska, materiella eller immateriella skador för enskilda (EDPB:s riktlinjer om anmälan av personuppgiftsincidenter enligt den allmänna dataskyddsförordningen, s. 24). Det kan till exempel handla om att det finns risk för skador i form av diskriminering, identitetsstöld eller bedrägeri (se även skäl 75 till dataskyddsförordningen).

Det främsta syftet med att informera de registrerade är att ge dem möjlighet att vidta åtgärder för att skydda sig från negativa konsekvenser som har orsakats av incidenten.

Vi ska lämna information till de registrerade om åtminstone:

- en beskrivning av incidentens art
- namnet på och kontaktuppgifterna till dataskyddsombudet eller annan kontaktpunkt,
- en beskrivning av de sannolika konsekvenserna av incidenten
- vad Försäkringskassan har gjort eller kommer att göra för att åtgärda incidenten, eller mildra negativa effekter av incidenten.

Vi behöver inte informera de registrerade om incidenten om vi har vidtagit åtgärder för att skydda de personuppgifter som påverkats av incidenten, till exempel om personuppgifterna har krypterats på ett sätt som gör dem oläsbara (artikel 34.3 a i dataskyddsförordningen).

Ett annat undantag från informationsskyldigheten är om åtgärder vidtagits efter att incidenten inträffat som innebär att risken för de registrerade inte längre är hög (artikel 34.3 b i dataskyddsförordningen).

15.3 Hur ska vi informera de registrerade?

Information om personuppgiftsincidenter ska i första hand lämnas direkt till de registrerade, till exempel genom mejl, sms eller post. Om direktkontakt med de registrerade skulle innebära en oproportionell ansträngning, till exempel för att det saknas kontaktuppgifter till dem, ska vi i stället informera allmänheten alternativt vidta en liknande åtgärd som informerar de registrerade på ett lika effektivt sätt (artikel 34.3 c i dataskyddsförordningen). Vi skulle till exempel kunna publicera en banderoll eller en framträdande informationsruta på vår webbplats. Vi ska välja den metod som maximerar chansen för registrerade att ta del av informationen.

Informationen ska ha en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med ett klart och tydligt språk (se avsnitt 11.1.4).

Läs mer
När vi lämnar information kan vi behöva beakta bestämmelser om sekretess och säkerhetskrav. Läs mer i Försäkringskassans vägledning (2001:3) Offentlighet, sekretess och utlämnande av handlingar och uppgifter och Försäkringskassans anvisningar (2022:09) Säkerhet på Försäkringskassan.

16 Överklagande, tillsyn och skadestånd

16.1 Överklagande av beslut enligt dataskyddsförordningen

7 kap. 2 § första och andra stycket i dataskyddslagen
Beslut enligt artiklarna 12.5 och 15–21 i EU:s dataskyddsförordning som har meddelats av en myndighet i egenskap av personuppgiftsansvarig får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Beslut som avser registrerades rättigheter kan överklagas till allmän förvaltningsdomstol. Andra beslut som vi fattar enligt dataskyddsförordningen får inte överklagas av en registrerad (7 kap. 5 § dataskyddslagen).

Överklagandet ska prövas av den förvaltningsrätt inom vars domkrets ärendet först har prövats (14 § lagen [1971:289] om allmänna förvaltningsdomstolar och 5 § förordningen [1977:937] om allmänna förvaltningsdomstolars behörighet m.m.). Om exempelvis ett beslut om avslag på en begäran om rättelse fattas i Östersund, ska Förvaltningsrätten i Härnösand pröva ärendet.

Ett överklagande omfattas av bestämmelserna i FL. Det innebär bland annat att överklagandet ska vara skriftligt och komma in till oss inom tre veckor från den dag då den registrerade fick del av beslutet genom oss (43–44 §§ FL). Vi är skyldiga att pröva om överklagandet har kommit in i rätt tid (45 § FL). Om överklagandet har kommit in i tid ska vi skyndsamt överlämna överklagandet och övriga handlingar till rätt domstol (46 § FL).

För ärendehanteringen i förvaltningsdomstol gäller bestämmelserna i förvaltningsprocesslagen (1971:291).

Läs mer
Läs mer om vad som gäller vid överklagande av beslut i Försäkringskassans vägledning (2001:7) *Omprövning och överklagande av Försäkringskassans beslut.*

16.2 IMY:s tillsyn

16.2.1 Klagomål till IMY

Artikel 77.1 i dataskyddsförordningen
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.

Den registrerade har möjlighet att lämna klagomål till IMY om hen tycker att hens

personuppgifter behandlas i strid med dataskyddsförordningen. Ett klagomål på Försäkringskassan kan leda till att IMY inleder tillsyn hos oss för att utreda klagomålet.

Det förekommer att IMY skickar klagomål till oss för kännedom. Syftet är att göra oss medvetna om att någon anser att Försäkringskassan behandlar personuppgifter på ett felaktigt sätt. Ibland kan klagomålet belysa en felaktighet som behöver åtgärdas.

16.2.2 Tillsyn

IMY är Sveriges nationella tillsynsmyndighet för behandling av personuppgifter och har som uppdrag att

- granska att dataskyddsrättsliga bestämmelser följs
- säkerställa att människors grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter.

IMY granskar genom att utföra tillsyn. Tillsynen kan vara klagomålsbaserad, riskbaserad eller årligen planerad. IMY genomför tillsyn antingen på plats (inspektion) eller genom att skicka frågor som ska besvaras skriftligen (skrivbordstillsyn).

IMY:s utredningsbefogenheter är långtgående och framgår av artikel 58.1 i dataskydds-förordningen. IMY har bland annat rätt att få

- tillgång till all information och alla personuppgifter som behövs för att genomföra tillsynen
- tillträde till våra lokaler och då få tillgång till all utrustning och alla andra medel för behandling av personuppgifter som vi använder.

16.2.3 Vad tillsynen kan leda till

För att se till att dataskyddsrättliga regler efterlevs har IMY ett antal korrigerande befogenheter. Det är åtgärder som kan riktas mot den som bryter mot eller riskerar att bryta mot reglerna. Åtgärderna är varning, reprimand, föreläggande, begränsning och förbud samt administrativa sanktionsavgifter.

IMY:s befogenheter gäller inte bara vid tillsyn över dataskyddsförordningens bestämmelser utan även andra föreskrifter som kompletterar dataskyddsförordningen, däribland 114 kap. SFB. Det framgår av 6 kap. 1 § dataskyddslagen.

Varning

IMY kan tilldela en skriftlig varning till en personuppgiftsansvarig eller ett personuppgifts-biträde om att planerade behandlingar sannolikt kommer att bryta mot dataskydds-rättsliga bestämmelser (artikel 58.2 a i dataskyddsförordningen). Det ska framgå av varningen på vilket sätt en behandling riskerar att strida mot bestämmelserna. En varning kan endast utfärdas innan en överträdelse ägt rum.

En varning kan kombineras med andra åtgärder, exempelvis förelägganden.

Reprimand

IMY kan utfärda en reprimand till en personuppgiftsansvarig eller ett personuppgifts-biträde om en behandling bryter mot dataskyddsrättsliga bestämmelser (artikel 58.2 b i dataskyddsförordningen). En reprimand är ett slags tillrättavisning och är en mildare åtgärd än sanktionsavgift. Den används bland annat vid mindre överträdelser (skäl 148 till dataskyddsförordningen).

Föreläggande

IMY kan besluta att den personuppgiftsansvariga eller ett personuppgiftsbiträde ska vidta en åtgärd (artikel 58.2 c, d, e, g, j i dataskyddsförordningen). Det kallas för ett föreläggande.

Ett föreläggande kan bland annat handla om att den personuppgiftsansvariga ska

- tillmötesgå den registrerades begäran att få utöva sina rättigheter enligt dataskyddsförordningen
- se till att behandlingen sker i enlighet med dataskyddsförordningen och om så krävs på ett specifikt sätt och inom en specifik period
- meddela den registrerade att en personuppgiftsincident har inträffat
- rätta eller radera personuppgifter
- begränsa behandling av personuppgifter.

Om vi inte följer ett föreläggande kan IMY besluta om sanktionsavgifter.

Begränsning och förbud mot behandling

IMY kan införa en tillfällig eller definitiv begränsning av en viss behandling av personuppgifter (artikel 58.2 f i dataskyddsförordningen). I praktiken kan det innebära att IMY förbjuder viss behandling.

Om vi inte rättar oss efter en begränsning kan IMY fatta beslut om sanktionsavgifter.

Administrativa sanktionsavgifter

6 kap. 2 § dataskyddslagen
Tillsynsmyndigheten får ta ut en sanktionsavgift av en myndighet vid överträdelser som avses i artikel 83.4, 83.5 och 83.6 i EU:s dataskyddsförordning, i den ursprungliga lydelsen. Då ska artikel 83.1, 83.2 och 83.3 i förordningen tillämpas.

Sanktionsavgiften ska bestämmas till högst 5 000 000 kronor vid överträdelser som avses i artikel 83.4 i EU:s dataskyddsförordning och till högst 10 000 000 kronor vid överträdelser som avses i artikel 83.5 och 83.6 i förordningen.

IMY kan besluta om att ta ut en sanktionsavgift av Försäkringskassan vid överträdelser av bestämmelser i dataskyddsförordningen. Sanktionsavgifter syftar till att stärka verkställigheten av dataskyddsförordningen (skäl 148 till dataskyddsförordningen). Vid beslut om administrativa sanktionsavgifter ska IMY säkerställa att det i varje enskilt fall är effektivt, proportionellt och avskräckande (artikel 83.1 i dataskyddsförordningen).

Vid beslut om sanktionsavgifter tar IMY hänsyn till överträdelsens karaktär, svårighetsgrad och varaktighet i förhållande till den aktuella personuppgiftsbehandlingens omfattning och syfte, kategorierna av personuppgifter, antalet berörda registrerade och den skada som de har lidit.

Rättsfall

Det har bedömts finnas skäl för att påföra sanktionsavgift när Spotify AB inte på ett tydligt och lätt tillgängligt sätt har lämnat den information som är nödvändig för att den registrerade ska kunna ta tillvara sina rättigheter enligt förordningen (artikel 12.1), inte har lämnat information om lagringsperioder och kriterier för fastställande av dessa (artikel 15.1 d) och inte har lämnat tillräcklig information om lämpliga skyddsåtgärder vid överföring av personuppgifter till ett tredje land eller en internationell organisation (artikel 15.2). (KRNS mål nr 4512-24)

Det har bedömts finnas skäl för att påföra sanktionsavgift när Klarna Bank AB inte har angett den rättsliga grunden för samtliga ändamål (artikel 13.1 c), inte har lämnat information om hur de registrerade kan få tillgång till information om skyddsåtgärder vid tredjelandsöverföringar (artikel 13.1 f), inte har lämnat fullständig information om hur personuppgifter kommer att lagras (artikel 13.2 a), inte har lämnat information om att en scoremodell används och vilka uppgifter som behandlas i denna (artiklarna 13.2 f och 14.2 g), samt lämnat otydlig eller svårtillgänglig information om tjänsten Min ekonomi, rätten till dataportabilitet, begränsning och automatiserat beslutsfattande (artikel 12.1). (KRNS mål nr 2829-23)

Det har bedömts finnas skäl att påföra sanktionsavgift för en nämnd i Stockholms kommun när det har funnits möjlighet att ta del av information i den så kallade Skolplattsformen utan behörighet. Informationen omfattade känsliga personuppgifter och även andra särskilt skyddsvärda uppgifter, som skyddade personuppgifter och uppgifter om elevomdömen. Behandlingen berörde ett mycket stort antal registrerade, till stor del barn. De registrerade eleverna kunde inte påverka behandlingen. Omständigheten att skadan för de registrerade var relativt begränsad medförde ingen annan bedömning. (KRNS mål nr 7837-21)

IMY har bedömt att det att funnits skäl att påföra en kommunal nämnd en administrativ sanktionsavgift för att nämnden inte hade genomfört en konsekvensbedömning. Konsekvensbedömningen skulle avse en behandling som omfattade 5 945 barn som i egenskap av elever befann sig i beroendeställning till den personuppgiftsansvarige. (IMY-2023-1647)

EU-domstolen har slagit fast att det krävs att överträdelsen har begåtts genom ett vållande, alltså uppsåtligen eller genom oaktsamhet, för att administrativa sanktionsavgifter ska kunna påföras (EU-domstolens domar Deutsche Wohnen, C-807/21, EU:C:2023:950, punkt 68 och 75 och Nacionalinis visuomenės sveikatos centras, C-683/21, EU:C:2023:949, punkt 73 och 80). Enligt Kammarrätten i Stockholm är det fråga om vållande om den personuppgiftsansvariga inte kan anses ha varit okunnig om att dess agerande inneburit överträdelser av dataskyddsförordningen (KRNS mål nr 2829-23).

De åtgärder som den som har orsakat en skada har vidtagit för att lindra den skada som de registrerade har lidit ska beaktas vid beslut om eventuell sanktionsavgift. Genom att snabbt vidta åtgärder vid en överträdelse kan vi alltså både minimera skadorna för den registrerade och minska risken för att IMY beslutar om en sanktionsavgift. Det är också viktigt att vi anmäler överträdelsen till IMY och samarbetar med IMY för att minska överträdelsens eventuella negativa effekter.

IMY beaktar även vilka tekniska och organisatoriska säkerhetsåtgärder vi har vidtagit. Ett medvetet säkerhetsarbete är därmed grundläggande för att både förebygga

överträdelser och undvika sanktionsavgifter om Försäkringskassan ändå gör sig skyldig till en överträdelse.

Försäkringskassan är ansvarig för behandling av personuppgifter som utförs av ett personuppgiftsbiträde. Detta innebär att Försäkringskassan kan påföras administrativa sanktionsavgifter för överträdelser som görs av ett biträde när det behandlar personuppgifter för vår räkning. Ansvaret omfattar dock inte behandling som sker i strid med biträdesavtalet. Det är därför viktigt att biträdesavtalet sätter tydliga ramar för behandlingen (se avsnitt 10.2).

Artikel 29-gruppen har gett ut riktlinjer om administrativa sanktionsavgifter (WP 253), som EDPB har ställt sig bakom. EDPB har dessutom gett ut riktlinjer (4/2022) om beräkningen av administrativa sanktionsavgifter.

16.3 Skadestånd

Den som lider materiell eller immateriell skada till följd av att Försäkringskassan behandlar personuppgifter i strid med dataskyddsförordningen kan ha rätt till skadestånd för den uppkomna skadan (artikel 82 i dataskyddsförordningen).

Rätten till ersättning gäller även vid behandling som strider mot dataskyddslagen, 114 kap. SFB och andra svenska föreskrifter som kompletterar dataskyddsförordningen (skäl 146 till dataskyddsförordningen och 7 kap. 1 § dataskyddslagen).

Den registrerade kan antingen väcka skadeståndstalan i allmän domstol eller begära skadestånd direkt från Försäkringskassan.

Läs mer

Läs om rätten till skadestånd i Försäkringskassans vägledning (2024:1) *Skadestånd och ersättning av allmänna medel*.

Källförteckning

EU-rätt

Europeiska unionens stadga om de grundläggande rättigheterna (rättighetsstadgan)

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

Kommissionens genomförandebeslut (EU) 2021/915 av den 4 juni 2021 om standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden enligt artikel 28.7 i Europaparlamentets och rådets förordning (EU) 2016/679 och artikel 29.7 i Europaparlamentets och rådets förordning (EU) 2018/1725

EU-domstolens domar

EU-domstolens dom Brillen Rottler GmbH & Co. KG mot TC, C-526/24, EU:C:2026:216

EU-domstolens dom Integritetsskyddsmyndigheten mot AB Storstockholms Lokaltrafik, C-422/24

EU-domstolens dom Deldits, C-247/23, EU:C:2025:172

EU-domstolens dom Mousse, C-394/23, EU:C:2025:2

EU-domstolens dom Másdi, C-169/23, EU:C:2024:988

EU-domstolens dom Lindenapotheke, C-21/23, EU:C:2024:846

EU-domstolens dom Schrems, C-446/21, EU:C:2024:834

EU-domstolens dom Endemol Shine Finland Oy, C-740/22, EU:C:2024:216

EU-domstolens dom IAB Europe, C-604/22, EU:C:2024:214

EU-domstolens dom SCHUFA Holding [Profilering], C-634/21, EU:C:2023:957

EU-domstolens dom Deutsche Wohnen, C-807/21, EU:C:2023:950

EU-domstolens dom Nacionalinis visuomenės sveikatos centras, C-683/21, EU:C:2023:949

EU-domstolens dom Österreichische Datenschutzbehörde och CRIF, C-487/21, EU:C:2023:369

EU-domstolens dom Meta Platforms m.fl., C-252/21, EU:C:2023:537

EU-domstolens dom Pankki S, C-579/21, EU:C:2023:501

EU-domstolens dom UZ, C-60/22, EU:C:2023:373

EU-domstolens dom Österreichische Datenschutzbehörde, C-487/21, EU:C:2023:369

EU-domstolens dom Vyriausioji tarnybinės etikos komisija, C-184/20, EU:C:2022:601

EU-domstolens dom Schrems II, C-311/18, EU:C:2020:559

EU-domstolens dom Latvijas Republikas Saeima, C-439/19, EU:C:2021:504

EU-domstolens dom Asociația de Proprietari bloc M5A-ScaraA, C-708/18, EU:C:2019:1064

EU-domstolens dom Jehovan todistatjat, C-25/17, EU:C:2018:551

EU-domstolens dom Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388

EU-domstolens dom Huber mot Tyskland, C-524/06, EU:C:2008:724

EU-domstolens dom Lindqvist, C-101/01, EU:C:2003:596

EDPB:s riktlinjer

EDPB, Riktlinjer 02/2026 om anonymisering

EDPB, Riktlinjer 9/2022 om anmälan av personuppgiftsincidenter enligt den allmänna dataskyddsförordningen, version 2.0, antagna den 28 mars 2023

EDPB, Riktlinjer 4/2022 om beräkningen av administrativa sanktionsavgifter, version 2.1, antagna den 24 maj 2023

EDPB, Riktlinjer 01/2022 om registrerades rättigheter – rätt till tillgång, version 2.1, antagna den 28 mars 2023

EDPB, Riktlinjer 05/2021 om samspelet mellan tillämpningen av artikel 3 och bestämmelserna om internationella överföringar enligt kapitel V i dataskyddsförordningen, version 2.0, antagna den 14 februari 2023

EDPB, Riktlinjer 01/2021 om exempel på anmälan av personuppgiftsincidenter, version 2.0, antagna den 14 december 2021

EDPB, Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, version 2.0, antagna den 7 juli 2021

EDPB, Riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679, version 1.1, antagna den 4 maj 2020

EDPB, Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter, version 2.0, antagna den 18 juni 2021

EDPB, Riktlinjer 4/2019 om artikel 25 Inbyggt dataskydd och dataskydd som standard, version 2.0, antagna den 20 oktober 2020

Artikel 29-gruppen, Riktlinjer om öppenhet (WP 260 rev. 01) enligt förordning 2016/679, antagna 29 november 2017, bekräftade av EDPB

Artikel 29-gruppen, 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), antagna den 4 oktober 2017, bekräftade av EDPB

Artikel 29-gruppen, Riktlinjer om administrativa sanktionsavgifter (WP 253), antagna den 3 oktober 2017, bekräftade av EDPB

Artikel 29-gruppen, Riktlinjer om dataskyddsombud (WP 243, rev. 01), antagna den 5 april 2017, bekräftade av EDPB

Artikel 29-gruppen, Yttrande 3/2013 om ändamålsbestämning enligt dataskyddsdirektivet (WP 203), i den engelska versionen, bekräftade av EDPB

Artikel 29-gruppen, Riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning [EU] 2016/679 (WP 251 rev. 01), antagna den 3 oktober 2017, bekräftade av EDPB

ENISA (EU:s cybersäkerhetsbyrå)

ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, Working Document, v1.0, December 2013

Konventioner

Den europiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen)

Svensk rätt

Grundlagar

Regeringsformen

Tryckfrihetsförordningen

Yttrandefrihetsgrundlagen

Lagar

Socialförsäkringsbalken

Lagen (2021:890) om skydd för personer som rapporterar missförhållanden

Lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter

Brottsdatalagen (2018:1177)

Säkerhetsskyddslagen (2018:585)

Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

Förvaltningslagen (2017:900)

Offentlighets- och sekretesslagen (2009:400)

Lagen (2008:145) om statligt tandvårdsstöd

Lagen (2001:99) om den officiella statistiken

Arkivlagen (1990:782)

Arbetsmiljölagen (1977:1160)

Förvaltningsprocesslagen (1971:291)

Lagen (1971:289) om allmänna förvaltningsdomstolar

Förordningar

Förordningen (2024:14) om behandling av personuppgifter vid Försäkringskassan och Pensionsmyndigheten

Förordningen (2022:524) om statliga myndigheters beredskap

Förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning

Förordningen (2009:1174) med instruktion för Försäkringskassan

Myndighetsförordningen (2007:515)

Förordningen (2001:100) om den officiella statistiken

Förordningen (1977:937) om allmänna förvaltningsdomstolars behörighet m.m.

Arkivförordningen (1991:446)

Rättsliga ställningstaganden

Försäkringskassans rättsliga ställningstagande (2025:04) Personuppgifter får vidarebehandlas utanför tillämpningsområdet för 114 kap. SFB

IMY:s rättsliga ställningstagande (IMYRS 2021:1) Innebörden av begreppet ”personuppgifter som rör lagöverträdelser som innefattar brott” i artikel 10 i dataskyddsförordningen

Förarbeten

Propositioner

Prop. 2024/25:180 Ökat informationsutbyte mellan myndigheter – en ny sekretessbrytande bestämmelse

Prop. 2024/25:157 Ett fritidskort för barn och unga – en aktiv och meningsfull fritid i gemenskap med andra

Prop. 2023/24:29 En ny dataskyddsreglering på socialförsäkringsområdet

Prop. 2020/21:193 Genomförande av visselblåsardirektivet

Prop. 2019/20:106 Stärkt integritet i Rättsmedicinalverkets verksamhet

Prop. 2017/18:298 Behandling av personuppgifter för forskningsändamål

Prop. 2017/18:232 Brottsdatalag

Prop. 2017/18:171 Dataskydd inom Socialdepartementets verksamhetsområde - en anpassning till EU:s dataskyddsförordning

Prop. 2017/18:107 Ändringar i vissa författningar inom Finansdepartementets ansvarsområde med anledning av EU:s dataskyddsreform

Prop. 2017/18:105 Ny dataskyddslag

Prop. 2017/18:95 Anpassningar av vissa författningar inom skatt, tull och exekution till EU:s dataskyddsförordning

Prop. 2009/10:85 Integritet och effektivitet i polisens brottsbekämpande verksamhet

Prop. 2009/10:7 Vissa ändringar i arbetslöshetsförsäkringen

Prop. 2008/09:70 Genomförande av tredje penningtvättsdirektivet

Prop. 2007/08:160 Utökat elektroniskt informationsutbyte

Prop. 2002/03:135 Behandling av personuppgifter inom socialförsäkringens administration

Statens offentliga utredningar

SOU 2017:39 Ny dataskyddslag. Kompletterande bestämmelser till EU:s dataskyddsförordning

SOU 2017:66 Dataskydd inom Socialdepartementets verksamhetsområde – en anpassning till EU:s dataskyddsförordning

SOU 2017:57 Lag om flygpassageraruppgifter i brottsbekämpningen

SOU 1999:105 Skatt - Tull - Exekution - Normer för behandling av personuppgifter

Nationella domar och beslut

Högsta domstolen

NJA 2005 s. 361

NJA 2025 s. 123 (I och II)

Högsta förvaltningsdomstolen

HFD mål nr Ä9385-25

HFD 2025 not 30

HFD 2025 not 13

HFD 2021 ref. 10

HFD 2020 not 16

HFD 2012 ref. 21

HFD mål nr 5118-21

HFD 2016 ref. 40

HFD 2015 ref. 61

HFD 2011 ref. 52

Kammarrätterna

Kammarrätten i Stockholm

KRNS mål nr 2452-25

KRNS mål nr 4512-24

KRNS mål nr 5794-23

KRNS mål nr 2829-23

KRNS mål nr 7385-22

KRNS mål nr 4058-22

KRNS mål nr 8588-21

KRNS mål nr 7837-21

KRNS mål nr 5888-20

Kammarrätten i Jönköping

KRNJ mål nr 2745-19

Justitiekanslern

JK:s beslut dnr 2023/9812, den 6 mars 2024

JK:s beslut dnr 2022/1169, den 11 april 2024

JK:s beslut dnr 3850-19-4.3.2, den 18 maj 2020

JK:s beslut dnr 2937-04-42, den 19 februari 2016

Försäkringskassans interna styr- och stöddokument

Generaldirektörens arbetsordning för Försäkringskassan, FK 2026/003942

Försäkringskassans säkerhetspolicy (2003:4)

Vägledningen (2024:1) Skadestånd och ersättning av allmänna medel

Vägledningen (2001:7) Omprövning och överklagande av Försäkringskassans beslut

Vägledningen (2001:3) Offentlighet, sekretess och utlämnande av handlingar och uppgifter

Riktlinjerna (2024:03) Bedöma och dokumentera personuppgiftsbehandlingar

Riktlinjerna (2019:01) Personuppgiftsbiträdesavtal

Riktlinjerna (2018:13) Säkerhetsregler

Riktlinjerna (2011:7) Utlämnande av allmänna handlingar och uppgifter

Anvisningarna (2025:19) Bedöma och dokumentera personuppgiftsbehandlingar

Anvisningarna (2025:17) Säkerhetsskydd

Anvisningarna (2023:07) Försäkringskassans visselblåsarfunktion

Anvisningarna (2022:09) Säkerhet på Försäkringskassan

Anvisningarna (2022:7) Hantering av säkerhetsincidenter

Integritetsskyddsmyndigheten (IMY)

IMY, Vägledning vid konsekvensbedömning, En praktisk guide, februari 2025

IMY, Vägledning vid konsekvensbedömning, Rättsligt tolkningsstöd, februari 2025

Förteckning enligt artikel 35.4 i dataskyddsförordningen, 2019-01-16, DI-2018-13200

IMY:s beslut, dnr IMY-2023-1647, 2023-11-28

IMY.se

Litteratur

Öman, *Dataskyddsförordningen [GDPR] m.m. En kommentar*, Norstedts juridik, JUNO Version 4

Brinnen m.fl., *Karnovs lagkommentar till dataskyddsförordningen*, JUNO Version 2026-07-01

Övrigt

eSams vägledning (ES2022-01) Pseudonymisering av personuppgifter