

Sammanträde i socialnämnden

Tid och plats för sammanträde

Onsdagen den 30 september 2020, kl. 09.00 B-salen, Västra Storgatan 15, Gnesta

Gruppmöten

Majoriteten (S, M); kl. 08.00. B-salen, Elektron. Oppositionen (C, L); kl. 08.00.
Frösjön/Lockvattnet, Elektron. Oppositionen (V, MP, Fi); kl. 08.00. Björken, Elektron.
Oppositionen (SD); kl. 08.00. Lokal, Elektron

Förslag till justerare

Ordinarie: Mari Klasson (C) Ersättare: Anne-Lise Ljung (SD)

Tid och plats för justering

Protokollet justeras i direkt anslutning till sammanträdet. Kommunledningskontoret
Västra Storgatan 15, Gnesta

Allmänheten

Allmänheten är välkommen att närvara vid sammanträdet.

Beslutsunderlag till ärendena i kallelsen finns på www.gnesta.se samt för läsning
digitalt på servicecenter.

Frågor om kallelsen och ärendena besvaras av sekreteraren, tel: 0158-275 000.

Dagordning

Sammanträdet öppnande samt upprop

Val av justerare och tid för justering

Godkännande av dagordningen

Offentliga 1 - 7, Ej offentliga 8 - 10

Nr	Diarienummer	Ärende
1	SN.2020.63	Remiss - SOU 2018:88 LSS-utredningen
2	SN.2020.22	Delegationsordning
3	SN.2020.73	Utse dataskyddsbud
4	SN.2020.65	Riktlinjer för tillämpning av dataskyddsförordningen

- | | | |
|----|--------------|--|
| 5 | SN.2020.32 | Rapportering av ej verkställda gynnande biståndsbeslut enligt SoL och LSS |
| 6 | SN.2020.1 | Redovisning av delegationsbeslut |
| 7 | SN.2020.2 | Anmälningsärenden |
| 8 | SN.2020.3 | Förvaltningschefen informerar |
| 9 | SN.2020.68 S | Väcka talan i tingsrätten avseende minderårig persons behov av särskild förordnad vårdnadshavare - Handlingar dukas på nämnden |
| 10 | SN.2020.69 S | Väcka talan i tingsrätten avseende minderårig persons behov av särskild förordnad vårdnadshavare - Handlingar dukas på nämnden |

Ingrid Jerneborg Glimne

Marie Solter

Ordförande

Sekreterare

Upprättad: 2020-09-16
Diarienummer: SN.2020.63

Socialnämnden

Remiss - SOU 2018:88 LSS-utredningen

Förslag till beslut i socialnämnden

1. Godkänner "Remissvar avseende SoU 2018:88 LSS-utredningen".

Sammanfattning

Gnesta kommun har mottagit en remiss från Regeringskansliet avseende SOU 2018:88 LSS-utredningen och har möjlighet att lämna synpunkter. Ett remissvar från Gnesta kommun har skrivits fram, se bilaga. Remissvaret ska ha inkommit till Regeringskansliet senast 2020-11-12.

Ärendebeskrivning

Ärendet har beretts av socialförvaltningen i samråd med barn- och utbildningsförvaltningen.

Jämställdhetsanalys utifrån checklista

Checklista för jämställdhet är inte tillämplig i ärendet.

Beslutsunderlag

1. Tjänsteskrivelse 2020-09-16
2. Remissvar avseende SoU 2018:88 LSS-utredningen

Veronica Östlin
Tf Förvaltningschef

Karin Pramlid
Utredare

Sändlista

- ~ Socialchef
- ~ Utredare, Soc kvalitetsteam
- ~ Barn- och utbildningsnämnden
- ~ Kommunstyrelsen

Remissvar avseende SOU 2018:88 LSS-utredningen

Inledning

Remissvaret är en gemensam skrivning från socialnämnden och barn- och utbildningsnämnden i Gnesta kommun. Svaret utgår från LSS-utredningens rubriksättning och innehåller de rubriker där vi har kommentarer.

Sammanfattning

Gnesta kommun ser både för- och nackdelar med utredningens förslag. Dock överväger nackdelarna och Gnesta kommun ställer sig negativ till utredningens förslag. Gnesta kommun anser att kostnaderna för kommunerna är lågt räknade och kommer troligtvis att bli ännu högre än vad utredningen angett. Utredningens beräkningsmodell samt de ekonomiska konsekvenserna för kommunerna behöver ytterligare förtydligas i utredningen.

De stora förändringar som föreslås i utredningen där insatsen personlig assistans samt assistansersättning för barn- och ungdomar upp till 16 år avvecklas och främst ersätts av en ny kommunal insats; personligt stöd till barn, innebär flera nackdelar för den enskilde och över tid ökade kostnader för kommunen. Utredningens inriktning att öka omsorgens utredningskapacitet och generella kompetens är välmenande, men svårt att realisera. Den nya föreslagna kommunala insatsen; förebyggande pedagogiskt stöd, som åsyftar att tillgodose det s.k. femte grundläggande behovet, det som förutsätter ingående kunskaper om den som får stödet, kommer fortsatt vara svårt att bedöma och leda till olika tolkningar. Den nya föreslagna kommunala insatsen; personlig service och boendestöd, innebär fördelar för den enskilde och ett utökat socialt ansvar för kommunen.

Bostaden

Utredningen föreslår en ny insats som ska kallas personlig service och boendestöd. Vi är positiva till insatsen boendestöd inkluderat ledsagning. Dock är vi tveksamma till förslaget att insatsen även ska gälla för särskilt boende. Utredningens förslag frångår den tidigare principen om att särskilt boende tillgodoser samtliga behov i boendesituationen. Insatsen blir svårt att bedöma och kommer att innebära olika tolkningar hos kommunerna. Förslaget om att insatsen även ska gälla särskilt boende kommer att innebära ökade kostnader för kommunerna.

Barn och familjer

Socialnämndens kommentarer

Utredningen föreslår att insatsen avlösarservice i hemmet istället ska benämnas avlösarservice för att det klart ska framgå att den inte är begränsad till att ges i hemmet. Vi är positiva till förändringen.

Personligt stöd i det dagliga livet

Barn- och utbildningsnämndens kommentarer

Givet utredningens förslag att korttidstillsyn för skolorngdom, oavsett benämningen, fortsätter vara en LSS-insats, är vi positiva till att insatsen byter namn till ett namn som bättre beskriver vad insatsen handlar om och samtidigt tydliggör skillnaden mellan insatsen och exempelvis korttidsvistelse. Vår bedömning är att benämningen "förlängd utbildning i fritidshem" uppfyller dessa krav. Vi är även positiva till att åldersgränsen för att beviljas insatsen justeras för att stämma överens med åldersgränsen för när plats i fritidshem inte längre beviljas.

Vidare föreslår utredningen att en framtida översyn av skollagen bör utreda huruvida insatsen ska regleras i skollagen istället. Detta är vi tveksamma till, med hänvisning till behovet av en tydlig ansvarsfördelning och att skolan behöver fokusera på sitt huvuduppdrag. Flyttas ansvaret till den nämnd vars verksamheter regleras av skollagen kan det få konsekvenser för verksamheten i stort.

Socialnämndens kommentarer

Utredningen föreslår att andra insatser än personlig assistans ska finnas för personer som behöver stöd som kräver ingående kunskaper. Vi är positiva till detta förslag.

Utredningen föreslår vidare att beredskap inte längre ska vara en del av den personliga assistansen och att sådant stöd kan ske på annat sätt, till exempel genom hemtjänst. Detta förslag är vi tveksamma till då detta kräver ständig beredskap av kommunen vad gäller personal med adekvat utbildning. Personalen behöver kunna behärska avancerade arbetsmoment (exempelvis andningsstöd) och utrustning inom detta område. Detta innebär svårigheter med rekrytering, men också kostnadsökningar för kommunen.

Utredningens förslag att det femte grundläggande behovet i personlig assistans ska tas bort och ersättas med personligt stöd för de med psykisk funktionsnedsättning kommer troligtvis leda till sämre kvalitet ur ett brukarperspektiv. Remissen föreslår att detta ska bli mer en hemtjänstliknande reform och hamna under SOL där det enligt lagtext står att individen har rätt till skäliga levnadsvillkor medan det i LSS står att individen har rätt till goda levnadsvillkor.

Vi är positiva till att utredningens förslag uppmärksammar den ökande andelen personer med funktionsnedsättningar som kräver särskilt ingående kunskaper. Vi är dock tveksamma till att kommunerna ska ansvara för dessa insatser. Insatsen kommer att vara helt assistanslik och leda till än mer omfattande volym när det exkluderas från annan assistans. Vi ser fortsatta svårigheter med att utreda och bedöma behovet av särskild kunskap hos personal. Detta kommer i sin tur att leda till olika tolkningar hos kommunerna och ojämlika möjligheter för de personer insatsförslaget berör.

Utredningen föreslår en ny kommunal insats; personligt stöd för barn; som ska gälla för barn och ungdomar under 16 år som på grund av stor och varaktig

funktionsnedsättning behöver hjälp i vardagen. Som en följd av detta förslag avslutas Försäkringskassans tidigare uppdrag att betala assistansersättning enligt SFB för barn och ungdom upp till 16 år. Vi ställer oss negativa till detta förslag som över tid kommer att leda till att kommunerna kommer att få högre kostnader.

Utjämning och fördelning av kostnader

Utredningen föreslår att staten blir ensam huvudman för insatsen personlig assistans. Vi ställer oss tveksamma till om utredningens förslag verkligen kommer att innebära en förändring och ett minskat ansvar för kommunerna. Flera av de ansvarsområden som kommunen har idag kring personlig assistans kommer fortfarande att återstå. Till exempel föreslås kommunerna fortsatt bekosta upp till 20 timmar/vecka till Försäkringskassan, kommunerna ansvarar fortsatt för att anordna assistans vid behov samt att det fortfarande går att välja insats från kommunen.

Konsekvenser av förslagen

Socialnämndens kommentarer

Utredningen uppskattar att kommunernas kostnader beräknas öka med mellan 300 miljoner och 400 miljoner kronor varje år. Förklaringen är ökade kostnader för de nya kommunala LSS-insatserna. Vi ställer oss tveksamma till detta då vi anser att kostnaderna för kommunerna är lågt räknade och kommer troligtvis att bli ännu högre än vad utredningen angett. Utredningens beräkningsmodell samt de ekonomiska konsekvenserna för kommunerna behöver ytterligare förtydligas i utredningen. Utredningens förslag kan i förlängningen innebära behov av skattehöjning för att kunna finansiera de nya kommunala LSS-insatserna.

Det är svårt att tydligt avgöra vad de nya LSS insatserna kommer innebära för kvaliteten. Vi kan dock konstatera att de kommer innebära en inskränkning på självbestämmanderätten för funktionsnedsatta. I och med att det blir kommunerna som ska bestämma över utförandet av de insatser som ska ersätta personlig assistans. Vi kommer se olika tolkningar vilket inte blir rättssäkert. På sikt kan det även innebära inlåsningseffekter. Individer som bor i en frikostig kommun kommer behöva ompröva sina beslut vid flytt till annan kommun. Den nya kommunen kanske inte gör samma bedömningar som den gamla hemkommunen, det främjar inte jämlikhet och delaktighet i samhället. Gnesta kommun önskar att utredningen fokuserar mer på kvaliteten för den enskilde. Förslagen innebär en försämring för den redan utsatta målgruppen och dess anhöriga.

Upprättad: 2020-08-21
Diarienummer: SN.2020.22

Socialnämnden

Delegationsordning revidering

Förslag till beslut i socialnämnden

1. Godkänna revideringen av delegationsordningen.

Ärendebeskrivning

Socialförvaltningen föreslår ändringar i form av 2 tillägg i delegationsordningens punkt 18.10 och 18.11. Tilläggen innebär att avgiftshandläggare, (Avg. handl.) får delegation att verkställa; jämkning av avgift för hemtjänst samt boende och beslut om nedskrivning av eller befrielse från skuld avseende debiterad avgift inom äldre- och handikappområdet. Bakgrunden är att effektivisera arbetsuppgifterna. Nedan syns ett utklipp från delegationsordningen på de tillägg som föreslås under punkt 18.10 och 18.11:

18.9	Beslut om avgift.	8 kap. 2 § SoL	VC Avg. <u>handl.</u> EC VC	
18.10	Jämkning av avgift för hemtjänst samt boende.	8 kap. 2 § SoL	Avg. <u>handl.</u> EC VC	
18.11	Beslut om nedskrivning av eller befrielse från skuld avseende debiterad avgift inom äldre- och handikappområdet.	4 kap. 2 § SoL	Avg. <u>handl.</u> FC EC,VC	

Socialförvaltningen föreslår också ett tillägg i delegationsordningen under avsnitt 2 som rör Offentlighets- och sekretesslagen samt GDPR. Tillägget är punkt 2.14 som innebär att förvaltningschefen har delegat att utse GDPR-samordnare. Nedan syns ett utklipp från delegationsordningen på det tillägg som föreslås:

2.14	Utse GDPR-samordnare	--	Förvaltningschef	
------	----------------------	----	------------------	--

Jämställdhetsanalys utifrån checklista

Förslag till beslut i ärendet bedöms inte få konsekvenser som leder till fördelar eller nackdelar för kvinnor/män och flickor/pojkar.

Beslutsunderlag

1. Tjänsteskrivelse 2020-08-21

Veronica Östlin
Förvaltningschef

Ida Claesson
Utredare

Sändlista

- ~ Patrik Rosin, Verksamhetschef AoB
- ~ Ida Claesson, Utredare, Socialförvaltningen

Upprättad: 2020-09-21
Diarienummer: SN.2020.73

Socialnämnden

Utse dataskyddsbud

Förslag till beslut i socialnämnden

1. Svitlana Jelisic utses till nämndens dataskyddsbud.

Ärendebeskrivning

Kommuner och deras självständiga nämnder är myndigheter och måste utse dataskyddsbud. Det är varje självständig nämnd som är personuppgiftsansvarig för behandlingar inom sitt verksamhetsområde och som ansvarar för att utse ett ombud.

Dataskyddsbudets roll att informera och ge råd till den personuppgiftsansvariga organisationen om vilka skyldigheter som gäller enligt dataskyddsförordningen. Ombudet ska också bevaka att reglerna följs samt fungera som kontaktperson för Datainspektionen.

Förvaltningens synpunkter

Jämställdhetsanalys utifrån checklista

Bedöms inte vara tillämplig i ärendet.

Överensstämmelse med kommunens styrdokument

Enligt artikel 37 i dataskyddsförordningen ska personuppgiftsansvarige utnämna ett dataskyddsbud.

Beslutsunderlag

1. Tjänsteskrivelse 2020-09-21

Veronica Östlin
Tf. förvaltningschef

Marie Solter
Nämndsekreterare

Sändlista

~ Datainspektionen

Upprättad: 2020-09-09
Diarienummer: SN.2020.65

Socialnämnden

Riktlinjer för tillämpning av dataskyddsförordningen

Förslag till beslut i samhällsbyggnadsnämnden

1. Riktlinjer för tillämpning av dataskyddsförordningen antas.
2. Förvaltningen får i uppdrag att ta fram rutiner för samtycke, registerutdrag, rättelse, radering, begränsning, invändning och dataportabilitet samt personuppgiftsincident.

Ärendebeskrivning

Dataskyddsförordningen eller The General Data Protection Regulation (GDPR) ersatte personuppgiftslagen (PUL) när den infördes 25 maj 2018. Förordningen innebär ett förstärkt skydd för den enskilda personens integritet.

För att kunna efterfölja dataskyddsförordningen har Strängnäs, Vingåkers, Flens, Katrineholms, Oxelösunds och Gnestas kommuner i samarbete tagit fram gemensamma riktlinjer för det fortsatta arbetet. Riktlinjerna antas av respektive personuppgiftsansvarige dvs. Respektive nämnd.

Förvaltningens synpunkter

Jämställdhetsanalys utifrån checklista

Dataskyddsförordningen gäller för alla levande personer oavsett kön. Personuppgifter om barn anses särskilt skyddsvärda i dataskyddsförordningen eftersom barn kan ha svårare att förutse riskerna med att lämna ifrån sig uppgifter och att förstå vilken rätt till skydd de har för sina uppgifter.

Överensstämmelse med kommunens styrdokument

Ett antagande av riktlinjerna för tillämpningen av dataskyddsförordningen är ett led i kommunens arbete med GDPR.

Beslutsunderlag

1. Tjänsteskrivelse 2020-09-09

2. Riktlinjer för tillämpning av dataskyddsförordningen

Veronica Östlin
TF. förvaltningschef

Sändlista

- ~ Kanslienheten
- ~ Dataskyddsombud

Riktlinjer för tillämpning av dataskyddsförordningen



Innehållsförteckning

1. Inledning	5
1.1 Bakgrund och syfte	5
1.2 Tillämpningsområde och omfattning	6
1.3 Definitioner	6
3. Dataskyddet i EU	8
4. Grundläggande principer	10
4.1 Laglighet	10
4.2 Korrekthet	10
4.3 Öppenhet	10
4.4 Ändamålsbegränsning	10
4.5 Uppgiftsminimering	11
4.6 Riktighet	11
4.7 Lagringsminimering	12
4.8 Integritet och konfidentialitet	12
4.9 Ansvarsskyldighet	12
5 Personuppgiftsansvarig	13
5.1 Vem är personuppgiftsansvarig?	13
5.2 Vad innebär det att vara personuppgiftsansvarig?	13
5.3 Utnämning av dataskyddsombud	14
6 Personuppgiftsbiträde	15
6.1 Vem är personuppgiftsbiträde?	15
6.2 Personuppgiftsbiträdesavtal	15
7 Dataskyddsombud	17
8 GDPR-samordnare	18
8.1 Utnämning av GDPR-samordnare	18
8.2 Kommunövergripande GDPR-samordnarens uppgifter och ansvar	18
8.3 GDPR-samordnarens uppgifter och ansvar	18
8.4 Samverkan mellan kommunerna	19
9 Personuppgifter	19
9.1 Vad är en personuppgift?	19
9.2 Känsliga personuppgifter	20
9.3 Personnummer och samordningsnummer, andra extra skyddsvärda personuppgifter	20
10. Behandling av personuppgifter	22
10.1 Vad är en behandling?	22
10.2 Behandling av känsliga personuppgifter	23
10.3 Behandling av personnummer och samordningsnummer	23
10.4 Behandla redan insamlade personuppgifter på ett nytt sätt	23



11. Rättslig grund för behandling av personuppgifter	25
11.1 Inledande om rättsliga grunderna och hur de används	25
11.2 Myndighetsutövning och uppgift av allmänt intresse	25
11.3 Rättslig förpliktelse	26
11.4 Avtal	26
11.5 Samtycke	27
Exempel på när samtycke kan användas och exempel på när samtycke inte får användas finns på datainspektionens hemsida.	28
11.6 Grundläggande intresse	29
12. Den registrerades rättigheter	30
12.1 Rätt till information	30
12.2 Registerutdrag	31
12.3 Rättelse	31
12.4 Radering	32
12.5 Begränsning av behandling	33
12.6 Rätt till dataportabilitet (överföring)	33
12.7 Rätt att göra invändningar	34
12.8 Automatiserat beslutsfattande eller profilering	34
12.9 Avgift	35
12.10 Beslut och överklagande	35
12.11 Klagomål	35
12.12 Skadestånd	35
13. Säkerhetsåtgärder, behörighetsstyrning och åtkomst, radering	36
14. Överföring till tredje land	37
14.1 Adekvat skyddsnivå	37
14.2 När får uppgifter annars överföras till tredje land?	38
14.1.1 Bindande företagsbestämmelser	38
14.1.2 Standardavtalsklausuler som EU-kommissionen har beslutat om	39
14.1.3 Uppförandekoder och certifieringsmekanismer	39
14.1.4 Rättsligt bindande instrument mellan myndigheter	39
14.1.5 Tillstånd från tillsynsmyndigheten	40
15. Konsekvensbedömning	41
15.1 Prövningen av om konsekvensbedömning ska göras	41
15.2.1 När ska en konsekvensbedömning göras?	41
15.2.2 När ska en konsekvensbedömning inte göras?	45
15.3 En eller flera behandlingar?	45
15.4 Konsekvensbedömningens innehåll	45
15.5 Inhämta synpunkter från de registrerade?	46
15.6 Ska konsekvensbedömningen offentliggöras?	47



15.7 Hur ska konsekvensbedömning följas upp?	47
15.8 Sammanfattande beskrivning av stegen	47
16. Personuppgiftsincident	48
17. Gallring	49
18. Checklista	50
Bilageförteckning	51
1. Länder som omfattas av GDPR	51
2. Register författningar och speciallagstiftning	51
3. Personuppgiftsbiträdesavtal	51



1. Inledning

1.1 Bakgrund och syfte

Den 25 maj 2018 började EU:s dataskyddsförordning gälla i Sverige och i EU:s andra medlemsstater, se BILAGA 1. Dataskyddsförordningen (även kallad GDPR) reglerar hur personuppgifter ska behandlas med syftet att skydda den enskildes (den registrerades) rättigheter. Följer kommunen inte dataskyddsförordningen finns det en risk att de registrerades personliga integritet kränks och att kommunens anseende skadas. Tillsynsmyndigheten kan också föreskriva höga sanktionsavgifter¹ och den registrerade kan ha rätt till skadestånd om kommunen behandlar personuppgifter i strid med bestämmelserna i dataskyddsförordningen.

Dataskyddsförordningen ersätter personuppgiftslagen och innebär bland annat att:

- Den personuppgiftsansvarige ska följa de grundläggande principerna.
- Den personuppgiftsansvarige ska informera de registrerade om behandlingar av deras personuppgifter.
- Rättigheterna för de registrerade i förhållande till den personuppgiftsansvarige utökas.
- Den personuppgiftsansvarige blir skyldig att visa att dataskyddsförordningen följs. Detta innebär en omfattande dokumentationsskyldighet (exempelvis krav på registerförteckning, konsekvensbedömning och gallringsrutiner).
- Missbruksregeln tas bort vilket betyder att även behandling av ostrukturerat material omfattas av dataskyddsförordningen.
- Kraftfulla sanktioner.

Flens kommun, Gnestas kommun, Katrineholms kommun, Strängnäs kommun, Oxelösunds kommun och Vingåkers kommun samarbetar kring dataskyddsförordningen.

Kommunerna har genom samarbetet utsett ett gemensamt dataskyddsombud samt tillsammans tagit fram dessa riktlinjer för tillämpning av dataskyddsförordningen

Syftet med riktlinjerna är att underlätta tillämpningen av dataskyddsförordningen. Riktlinjerna riktar sig till alla medarbetare som tillämpar dataskyddsförordningen i sitt dagliga arbete.

Riktlinjerna är ett levande dokument som ska uppdateras löpande vid nya rekommendationer, förändrat regelverk och ny praxis. Riktlinjerna är baserade på dataskyddslagstiftningen, såsom:

- [Dataskyddsförordningen](#).
- [Dataskyddsförordningens beaktandesatser \(skäl\)](#).
- Artikel 29-gruppens uttalanden (läs mer om artikel 29-gruppen i avsnitt 3).

¹ För kommunens personuppgiftsansvariga kan avgiften uppgå till 10 miljoner kronor. Kommunala bolag kan bli skyldiga att betala en sanktionsavgift på upp till tjugo miljoner euro eller 4 % av den totala globala årsomsättningen, beroende på vilket värde som är högst.



- [Lag \(2018:218\) med kompletterande bestämmelser till EU:s dataskyddsförordning \(dataskyddslagen\).](#)
- [Förordning \(2018:219\) med kompletterande bestämmelser till EU:s dataskyddsförordning](#)
- Registerförfattningar som gäller inom olika områden, som till exempel inom socialförvaltningen, läs mer i BILAGA 2.

1.2 Tillämpningsområde och omfattning

Riktlinjer gäller för personuppgiftsansvariges anställda, förtroendevalda och konsulter/uppdragstagare, på alla marknader och vid var tid.

Personuppgiftsansvariges ledning ska se till att riktlinjerna följs, vilket bland annat innefattar utbildning för anställda och förtroendevalda. Informationen till de anställda ska även innefatta information om att överträdelse av riktlinjerna kan komma att medföra t ex arbetsrättsliga konsekvenser.

I dessa riktlinjer lämnas exempel på viss dokumentation som bör upprättas och här återfinns också närmare information om de legala kraven.

1.3 Definitioner

Nedan definieras en rad begrepp och ord som används i dessa riktlinjer.

Behandling av personuppgifter - Åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller inte, 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. Läs mer om behandling av personuppgifter under kap. 10.

Dataskyddslagstiftning - Lagar och förordningar på dataskyddsområdet som har kommit till för att skydda den enskildes personliga integritet. Läs mer om dataskyddslagstiftningen under kap. 3.

Incidentgrupp - en grupp anställda inom kommunen som hanterar personuppgiftsincidenter. Incidentgruppen kan bestå av IT-chef, säkerhetsansvarig, jurist, dataskyddsombud och GDPR samordnare. Läs mer om incidentgruppen under kap. 8.2 och 16.

Konsekvensbedömning avseende dataskydd - konsekvensbedömning ska göras om en ny eller ändrad personuppgiftsbehandling kan komma att medföra en hög risk för fysiska personers rättigheter och friheter. Särskilda risker för fysiska personers rättigheter och friheter kan exempelvis förekomma i samband med behandling av känsliga uppgifter, behandling i särskilt stor omfattning eller vid användning av ny teknik. Läs mer om konsekvensbedömning under kap. 15.



Personuppgiftsansvarig - Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Varje kommunstyrelse och varje nämnd är personuppgiftsansvariga inom den kommunala verksamheten. Läs mer om personuppgiftsansvarig under kap. 5.

Personuppgiftsbiträde - Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Personuppgiftsansvariga ska upprätta personuppgiftsbiträdesavtal med personuppgiftsbiträdena. Läs mer om personuppgiftsbiträdesavtal under kap. 6.

Personuppgifter - Varje upplysning som avser en identifierad eller identifierbar fysisk person (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 lokaliseringssuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet. Läs mer om personuppgifter under kap. 9.

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 behandlas. Läs mer om personuppgiftsincident under kap. 16.

Registrerad - en fysisk levande person som personuppgiften avser.

Registerutdrag - Den registrerade har rätt att få information om huruvida dennes personuppgifter behandlas, och i sådana fall få en kopia av personuppgifterna (*registerutdrag*). Läs mer om registerutdrag under kap. 12.2.

Tredje land - En stat som inte ingår i Europeiska unionen (EU) eller är ansluten till Europeiska ekonomiska samarbetsområdet (EES). Se BILAGA 1. Vilka länder omfattas av dataskyddsförordningen.

Överföring till tredje land - Överföring av personuppgifter till länder utanför EU och EES (så kallad tredjelandsöverföring). Det kan till exempel handla om online IT-tjänster, molnbaserade tjänster, tjänster för extern åtkomst eller globala databaser. Tredjelandsöverföring får endast ske under särskilda förutsättningar. Läs mer om detta under kap. 14.

Underbiträde - Ett personuppgiftsbiträde som anlitas av det personuppgiftsbiträdet som har ett personuppgiftsbiträdesavtal med den personuppgiftsansvarige och som också behandlar personuppgifter för personuppgiftsansvariges räkning. Underbiträdet har samma skyldigheter gällande behandling av personuppgifter som personuppgiftsbiträdet.



3. Dataskyddet i EU

Nationella dataskyddsmyndigheter (DPA) - Inom EU har respektive land sin egen nationella dataskyddsmyndighet. I Sverige är det Datainspektionen, i Danmark Datatilsynet, i Finland Dataombudsmannens byrå och så vidare. På engelska brukar dessa kallas för DPA:s, Data Protection Authorities.

I Sverige ska tillsynsmyndigheten se till att myndigheter, kommuner, företag och andra organisationer följer dataskyddsförordningen, den svenska kompletterande dataskyddslagen, brottsdatalagen och kamerabevakningslagen. Den svenska tillsynsmyndigheten ska dessutom kunna begära hjälp av systemmyndigheter i andra EU-länder vid granskningar av gränsöverskridande verksamheter. Den svenska tillsynsmyndigheten kommer att byta namn från Datainspektionen till Integritetsskyddsmyndigheten.

Artikel 29-gruppen - Den 24 oktober 1995 antog EU ett direktiv om skydd för enskilda personer med avseende på behandling av personuppgifter. Direktivet ledde senare fram till den svenska personuppgiftslagen. För att direktivet ska tillämpas på ett enhetligt sätt i medlemsstaterna har den så kallade artikel 29-gruppen bildats. Gruppen har fått sitt namn av artikel 29 i dataskyddsdirektivet och i artikel 30 finns bestämmelser om gruppens uppgifter. Gruppen är rådgivande och oberoende och ska se till att direktivet tillämpas enhetligt i medlemsstaterna. Arbetsgruppen består av företrädare för varje nationell tillsynsmyndighet i EU-medlemsstaterna, för EU-kommissionen samt den europeiska datatillsynsmannen. Bland andra Norge, Island, Liechtenstein och Kroatien deltar som observatörer.

Den 25 maj 2018 upphörde Artikel 29-gruppen som då ersattes av den Europeiska dataskyddsstyrelsen.

Europeiska dataskyddsstyrelsen (EDPB) - EDPB, European Data Protection Board, eller Europeiska dataskyddsstyrelsen, inrättades när dataskyddsförordningen började tillämpas i maj 2018. Den består av representanter från samtliga EU-länders dataskyddsmyndigheter, däribland tillsynsmyndigheten i Sverige. Styrelsen har befogenhet att fatta beslut i frågor där nationella tillsynsmyndigheter inte kan komma överens, ge råd och vägledning om hur dataskyddsförordningen ska tillämpas och godkänna EU-omfattande uppförandekoder och certifieringar.

Europeiska datatillsynsmannen (EDPS) - Europeiska datatillsynsmannen eller European Data Protection Supervisor som förkortas EDPS. I EU finns det myndigheter och institutioner som inte hör till något enskilt land. Det europeiska smittskyddsinstitutet ECDC är ett sådant exempel. Även om det är baserat i Solna strax utanför Stockholm så är det inte den svenska dataskyddslagstiftningen som reglerar hur ECDC får hantera personuppgifter. I stället måste ECDC följa en speciell EU-förordning, en sorts EU-personuppgiftslag, som bara gäller för EU:s institutioner och myndigheter. Den Europeiska datatillsynsmannens roll är att säkerställa att ECDC och andra EU-myndigheter följer reglerna i den lagstiftningen.



Svenska domstolar - Tillsynsmyndighetens beslut kan överklagas till domstol. I dataskyddsförordningen finns särskilda bestämmelser för när man kan vända sig till domstol för att få ett ärende prövat. Enskilda som anser att någon behandlar hans eller hennes personuppgifter i strid med förordningen eller annan lag kan också vända sig till domstol, till exempel för att begära rättelse eller för att kräva skadestånd.

EU-domstolen - EU-domstolen är den domstol som slutligen tolkar hur dataskyddsförordningen och annan EU-rätt ska tolkas och tillämpas. Om en nationell domstol är osäker på hur en lag ska tolkas kan den be EU-domstolen om råd genom att begära ett förhandsavgörande. Domstolen svarar då på de frågor som den nationella domstolen har ställt. Målet avgörs dock av den nationella domstolen.

Europadomstolen - Om en enskild individ anser att staten har kränkt hans eller hennes rättigheter enligt Europakonventionen är det i första hand svenska domstolar eller myndigheter som ska pröva om en kränkning har ägt rum, först därefter kan man ta ett klagomål vidare till Europadomstolen. Europadomstolen kan döma ut ett skadestånd till klaganden men kan inte upphäva en dom eller ett beslut som fattats av en nationell myndighet eller domstol.



4. Grundläggande principer

I dataskyddsförordningen finns ett antal grundläggande principer som kan sägas vara kärnan i förordningen. När personuppgifter behandlas ska de grundläggande principerna följas. Det är den personuppgiftsansvarige som är ansvarig för att visa att de har följts. Nedan följer en genomgång av de grundläggande principerna.

4.1 Laglighet

Laglighet innebär först och främst att personuppgiftsansvarige måste ha en rättslig grund för varje personuppgiftsbehandling. I dataskyddsförordningen finns sex rättsliga grunder för behandling av personuppgifter. Dessa är avtal, rättslig förpliktelse, myndighetsutövning eller uppgift av allmänt intresse, berättigat intresse, grundläggande intresse eller samtycke. Läs mer om rättsliga grunder under kap. 11. Det är endast tillåtet att behandla personuppgifter om det går att identifiera en rättslig grund som är tillämplig för behandlingen. Den grundläggande principen laglighet innebär också att personuppgiftsansvarige måste följa övriga principer och bestämmelser i dataskyddsförordningen och i annan kompletterande lagstiftning.

4.2 Korrekthet

Korrektthet innebär att behandlingen av personuppgifter ska vara rättvis, skälig, rimlig och proportionerlig i förhållande till de registrerade. Personuppgiftsbehandlingen ska stå i rimlig proportion till den nytta som personuppgiftsbehandlingen innebär. Det betyder att personuppgiftsansvarige ska väga sina egna intressen mot de registrerades innan personuppgifterna behandlas. Personuppgiftsansvarige ska också ta hänsyn till vilken personuppgiftsbehandling de registrerade rimligen kan förvänta sig.

4.3 Öppenhet

Principen om öppenhet innebär att det ska vara klart och tydligt för de registrerade hur personuppgiftsansvarige behandlar deras personuppgifter. Personuppgiftsbehandlingen ska vara förståelig och begriplig för de registrerade och inte ske på dolda eller manipulerande sätt. De registrerade ska alltså veta att den personuppgiftsansvarige samlar in personuppgifter, varför den samlar in dem och hur uppgifterna sedan används. De registrerade ska också veta vad de har för rättigheter, till exempel hur de kan begära registerutdrag, hur de kan få fel rättade och hur de kan få personuppgifter raderade. De registrerade måste därför få information om allt detta. Informationen ska vara lätt att hitta och den ska vara formulerad på ett sätt som är enkelt och begripligt. Det är särskilt viktigt att använda ett klart och tydligt språk om de registrerade är barn.

4.4 Ändamålsbegränsning

Personuppgifter får endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Personuppgiftsansvarige måste därför ha klart för sig varför personuppgifterna ska behandlas redan innan insamlingen sker. Ändamålen sätter ramarna för vad



personuppgiftsansvarige får och inte får göra, till exempel vilka uppgifter som får behandlas och hur länge de får sparas. Tänk på att:

- Ändamålen måste vara specifika och konkreta, inte luddiga eller otydliga. Det är till exempel inte tillräckligt att ange “kontroller” som ändamål för loggning och övervakning, utan att också ange syftet med kontrollen. Syftet med kontrollen är kanske övervakning av säkerhets- eller tekniska skäl eller uppföljning av interna regler. Det räcker normalt inte heller att ange ändamål som enbart är att “förbättra användarnas upplevelse”, “IT-säkerhet” eller “framtida forskning”. Det är alltför brett uttryckt, och de registrerade kan inte bedöma vad sådan personuppgiftsbehandling kan innebära.
- Ändamålet måste också vara berättigat. Detta innebär att personuppgiftsbehandlingen dels ska ha en rättslig grund i dataskyddsförordningen, dels ska ske i enlighet med övrig tillämplig lagstiftning och allmänna rättsprinciper.
- De registrerade har rätt att känna till varför deras personuppgifter behandlas, alltså vilka ändamålen är. Personuppgiftsansvarige informerar de registrerade om ändamålet när uppgifterna samlas in och även när en registrerad begär det.
- Personuppgiftsansvarige ska dokumentera vilka ändamål den har med personuppgiftsbehandlingen.
- Om insamlade personuppgifter ska behandlas på ett nytt sätt måste det vara förenligt med de ursprungliga ändamålen. I sådana fall kan personuppgiftsansvarige använda samma rättsliga grund som vid insamlingen av personuppgifterna.

4.5 Uppgiftsminimering

Personuppgifter som behandlas ska vara adekvata, relevanta och inte alltför omfattande i förhållande till ändamålen. Säkerställ att uppgifterna som samlas in verkligen behövs och fråga inte efter information bara för att den kanske kan vara bra att ha.

4.6 Riktighet

Personuppgifter som behandlas ska vara korrekta och om nödvändigt uppdaterade. Personuppgiftsansvarige ska vidta lämpliga åtgärder för att se till att felaktiga eller ofullständiga uppgifter rättas, exempelvis gällande ändring av adress vid flytt med en sammanställning av system och register där adressen lagras. Man ska dock inte lagra kopior av uppgifterna i många system i syfte att undvika felkällor och att icke uppdaterad information sparas.



4.7 Lagringsminimering

Personuppgifter får inte lagras under längre tid än nödvändigt med hänsyn till ändamålen med behandlingen. När uppgifterna inte längre behövs måste dessa gallras, vilket innebär att de antingen måste raderas eller avidentifieras. Vi får bara spara personuppgifter så länge som de behövs för ändamålet med personuppgiftsbehandlingen. När vi får gallra en viss typ av handling framgår av kommunstyrelsens eller nämndens dokumenthanteringsplan.

Personuppgifter som förekommer i handlingar som inte är allmänna handlingar ska raderas eller avidentifieras när de inte längre behövs. Vi får lagra personuppgifter efter det att det ursprungliga ändamålet slutar att vara aktuellt, om det sker för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Vi får alltså skicka handlingar som innehåller personuppgifter till kommunarkivet, trots att det ursprungliga ändamålet inte längre är aktuellt.

4.8 Integritet och konfidentialitet

Personuppgiftsansvarige måste skydda alla personuppgifter som den behandlar, så att ingen obehörig kommer åt dem och så att uppgifterna inte används på ett otillåtet sätt.

Personuppgiftsansvarige ska också se till så att personuppgifter inte förloras eller blir förstörda, till exempel genom olyckshändelser. Personuppgiftsansvarige måste därför införa lämpliga tekniska och organisatoriska säkerhetsåtgärder. Till tekniska åtgärder räknas till exempel brandväggar, kryptering, pseudonymisering, säkerhetskopiering och anti-virus-skydd. Organisatoriska åtgärder handlar till exempel om interna rutiner, instruktioner och riktlinjer.

4.9 Ansvarsskyldighet

Den grundläggande principen om ansvarsskyldighet innebär att personuppgiftsansvarige måste kunna visa att dataskyddsförordningen följs. Personuppgiftsansvarige måste därför exempelvis dokumentera arbetet gällande dataskydd. Vidare ska det finnas register över alla typer av behandlingar av personuppgifter som utförs och personuppgiftsansvarige ska kunna redovisa ett sådant register för tillsynsmyndigheten när så krävs.

Personuppgiftsansvarige ska visa att denne följer de grundläggande principerna på flera sätt, till exempel genom att:

- Lämna tydlig information till de registrerade
- Föra register över och dokumentera de personuppgiftsbehandlingar som pågår hos personuppgiftsansvarige
- Upprätta en dataskyddspolicy och utbilda personalen
- Bygga in integritetsvänliga lösningar i sina system (så kallat inbyggt dataskydd)
- Göra en konsekvensbedömning innan personuppgiftsansvarige påbörjar personuppgiftsbehandling som innebär särskilda integritetsrisker
- Utse ett dataskyddsbud.



5 Personuppgiftsansvarig

5.1 Vem är personuppgiftsansvarig?

Personuppgiftsansvarig är den organisation (till exempel aktieföretag, stiftelse, förening eller myndighet) som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till. Det är alltså inte chefen på en arbetsplats eller en anställd som är personuppgiftsansvarig.

Personuppgiftsansvariga inom kommuner är kommunstyrelsen och övriga nämnder.

Om två eller flera gemensamt bestämmer över en viss behandling är de personuppgiftsansvariga tillsammans och måste sinsemellan bestämma vem som är ansvarig för att fullgöra de olika skyldigheterna i dataskyddsförordningen.

Vem som är personuppgiftsansvarig kan också anges i lag eller förordning, till exempel i särskilda registerlagar.

Exempel: I 2 kap. 6 § patientdatalagen står det att i en kommun är varje myndighet, som bedriver hälso- och sjukvård, personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

5.2 Vad innebär det att vara personuppgiftsansvarig?

Den personuppgiftsansvarige måste se till att all personuppgiftsbehandling sker i enlighet med dataskyddslagstiftningen.

Den personuppgiftsansvarige har ett generellt ansvar att, utifrån de integritetsrisker som finns med behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen. Detta kan bland annat innebära att man har antagit en policy med lämpliga strategier för dataskydd och ser till att genomföra den i organisationen. Den grundläggande regleringen om detta finns i artikel 24 dataskyddsförordningen.

Den som är personuppgiftsansvarig kan överlåta den faktiska behandlingen av personuppgifter men personuppgiftsansvaret kan aldrig överlåtas.

Exempel: En enskild medarbetare som arbetar för kommunstyrelsen informerar inte om en personuppgiftsincident som den upptäckt (meddelar inte incidentgruppen). Datainspektionen har uppmärksammat detta. Kan Datainspektionen då begära att medarbetaren betalar sanktionsavgiften, eftersom det är medarbetaren som gjort fel? Nej, det är kommunstyrelsen som är personuppgiftsansvarig och som hålls ansvarig. Det är alltså kommunstyrelsen som ska betala sanktionsavgiften.



5.3 Utnämning av dataskyddsbud

I dataskyddslagstiftningen ställs det krav på att alla myndigheter ska utse ett så kallat dataskyddsbud. Det innebär att i kommunen måste kommunstyrelsen och varje nämnd utse ett dataskyddsbud. Det finns inget motsvarande krav för de kommunala bolagen. Med hänsyn till att dataskyddsfrågorna har kommit att få alltmer fokus finns det anledning att utse ett dataskyddsbud som ansvarar för frågor om integritetsskydd vid behandling av personuppgifter även inom de kommunala bolagen. Kommunala bolag bör därför utse ett dataskyddsbud.

Anmälan till tillsynsmyndigheten av dataskyddsbudet enligt artikel 37.7 i dataskyddsförordningen ska göras så snart det är möjligt för kommunstyrelse, nämnder och kommunala bolag. Det är den personuppgiftsansvarige som anmäler dataskyddsbud till tillsynsmyndigheten.

Den personuppgiftsansvarige har alltid det yttersta ansvaret gentemot tillsynsmyndigheten och de registrerade för att personuppgifter i verksamheten behandlas på ett lagligt och korrekt sätt och i enlighet med god sed.

För att dataskyddsbudets arbetsuppgifter ska kunna utföras på ett tillfredsställande sätt ska den personuppgiftsansvarige hålla dataskyddsbudet underrättad om vilka personuppgiftsbehandlingar som sker och de säkerhetsrutiner som skyddar personuppgifterna.

Personuppgiftsansvarig ska i god tid rådgöra med dataskyddsbudet innan förändringar av hantering och rutiner kring personuppgifter eller utvecklingsprojekt, som involverar personuppgifter, beslutas. Den personuppgiftsansvarige ska underrätta ombudet vid förfrågningar och klagomål från registrerade och andra externa parter, så som exempelvis kunder och media. Personuppgiftsansvarig ska stödja dataskyddsbudets arbete bland annat genom att ge denne tillgång till dokumentation och IT-system i den utsträckning som behövs.



6 Personuppgiftsbiträde

6.1 Vem är personuppgiftsbiträde?

Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges organisation. Ett personuppgiftsbiträde kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ. Den grundläggande regleringen om personuppgiftsbitrådets roll finns i artikel 4 och artikel 28 dataskyddsförordningen.

De biträden som den personuppgiftsansvarige anlitar ska kunna ge tillräckliga garantier för att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas.

Ett personuppgiftsbiträde och dess personal får enbart behandla personuppgifter enligt instruktion från den personuppgiftsansvarige. Bitrådet får inte anlita ett annat biträde utan att i förhand få ett skriftligt tillstånd av den personuppgiftsansvarige.

En nyhet i förordningen är att några av de skyldigheter som tidigare har gällt för den personuppgiftsansvarige nu även gäller för personuppgiftsbitrådet, till exempel kraven på att föra register över behandlingar, att säkerställa en lämplig säkerhetsnivå och att i vissa fall utse ett dataskyddsbud.

Även personuppgiftsbitrådet kan bli föremål för tillsyn eller administrativa sanktionsavgifter och bli skadeståndsansvarig.

Ibland kan det vara svårt att bedöma vem som är personuppgiftsbiträde och vem som är personuppgiftsansvarig. När det ska avgöras vem som har vilken roll utgår man ifrån vem det är som bestämmer hur personuppgifterna kommer att behandlas och varför de behandlas. Det är den organisationen/personen som är personuppgiftsansvarig.

6.2 Personuppgiftsbiträdesavtal

Den personuppgiftsansvarige och personuppgiftsbitrådet måste upprätta ett så kallat personuppgiftsbiträdesavtal. Dataskyddsförordningen räknar upp vad ett sådant biträdesavtal ska innehålla:

- Föremålet för behandlingen samt behandlingens art och ändamål
- Behandlingens varaktighet (tillsvidare eller tidsbestämt).
- Vilka kategorier av personuppgifter som ska hanteras, till exempel känsliga och/eller extra skyddade personuppgifter och eventuellt var de finns.
- Vilka kategorier av registrerade som ska hanteras (anställda, invånare, patienter, elever etc.).
- Personuppgiftsansvariges skyldigheter och rättigheter.



- Hänvisning till tillräckliga garantier (man får endast anlita biträden som kan ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder).
- Instruktioner om hur personuppgiftsbiträdet får behandla personuppgifterna.
- Om personuppgifterna får överföras till tredjeland och under vilka förutsättningar det i så fall får ske.
- Personuppgiftsbiträdes personal med behörighet att behandla våra personuppgifter ska ha tystnadsplikt. Det gäller även harmlös information.
- Personuppgiftsbiträdet ska vidta alla säkerhetsåtgärder som krävs enligt artikel 32 i dataskyddsförordningen.
- Personuppgiftsbiträde ska hjälpa till så att personuppgiftsansvarige kan fullgöra sina skyldigheter.
- Vad som händer med personuppgifterna när avtalet avslutas. Beroende på vad personuppgiftsansvarige väljer ska alla personuppgifter antingen raderas eller återlämnas och alla befintliga kopior ska raderas, så länge inte lagringen krävs enligt unionsrätten eller svensk lagstiftning.
- Personuppgiftsansvariges rätt till information om personuppgiftsbiträdets behandling av personuppgifterna.
- Personuppgiftsbiträdets skyldighet att bidra till granskningar och inspektioner som genomförs av den personuppgiftsansvarige eller av en revisor som har utsetts av den personuppgiftsansvarige.

Därutöver måste personuppgiftsbiträdet få ett särskilt eller allmänt skriftligt förhandstillstånd av personuppgiftsansvarige innan personuppgiftsbiträdet anlitar underbiträden. Till personuppgiftsavtalet bör det därför finnas en bilaga med de underbiträden som personuppgiftsbiträdet vet kommer att hantera personuppgiftsansvarigs personuppgifter.

Hur det ska gå till när personuppgiftsbiträdet vill byta ut eller anlita ett nytt underbiträde ska regleras i personuppgiftsbiträdesavtalet. Personuppgiftsbiträdet är skyldigt att se till att underbiträdet åläggs samma skyldigheter i fråga om dataskydd som personuppgiftsbiträdet har gentemot personuppgiftsansvarig. Personuppgiftsbiträdet ansvarar fullt ut gentemot personuppgiftsansvarig för sina underbiträden.

Det är den personuppgiftsansvarige som ska se till att personuppgiftsbiträdesavtal upprättas. En mall för personuppgiftsbiträdesavtal finns i BILAGA 3 och på SKR:s hemsida, vid uppdatering av avtalet på SKR:s hemsida ska senaste versionen av SKR:s avtal användas. Denna mall ska användas när kommunstyrelsen eller nämnden tecknar ett personuppgiftsbiträdesavtal.

Det är viktigt att alla personuppgiftsbiträdesavtal dokumenteras och är sökbara. Personuppgiftsbiträdesavtalet ska därför registreras i ett diariesystem eller på annat sätt hållas ordnat tillsammans med huvudavtalet. Ett personuppgiftsbiträdesavtal ska registreras i ett diariesystem som "Personuppgiftsbiträdesavtal".



7 Dataskyddsbud

Dataskyddsbudet utses av personuppgiftsansvarig och ombudets arbetsuppgifter inom de samarbetskommuner som denna vägledning omfattar att:

- Vara ett kunskapsstöd inom kommunerna gällande dataskyddsförordningen och annan tillämplig dataskyddslagstiftning.
- Övervaka den interna efterlevnaden av dataskyddsförordningen och annan tillämplig dataskyddslagstiftning
- Tillsammans med sakkunniga inom respektive kommun kravställa och arbeta för att införa säkerhetsåtgärder inom dataskydd.
- Bistå i utredning av misstänkt dataintrång.
- Ge råd vid konsekvensbedömningar av dataskydd och övervaka genomförandet av dem.
- Arbeta med omvärldsbevakning kunskapsinhämtning rörande dataskyddslagstiftning.

Dataskyddsbudet har inget personligt ansvar för att alla anställda och förtroendevalda följer reglerna i dataskyddslagstiftningen. Om dataskyddsbudet anser att en behandling av personuppgifter inom ombudets ansvarsområde förs i strid med dataskyddslagstiftningen, ska dataskyddsbudet påtala detta för berörd chef. Dataskyddsbudet är inte den som slutligen avgör hur personuppgifter ska hanteras utan har en rådgivande och reviderande roll.

Dataskyddsbudet har enligt dataskyddslagstiftningen en självständig ställning gentemot personuppgiftsansvarige, som kan jämföras med en internrevisors. Flens kommun har huvudansvaret för dataskyddsbudets arbetssituation och ska se till att denne har tillräckligt med tid, kompetens och resurser för att genomföra sin ombudsroll på ett tillfredsställande sätt.

Dataskyddsbudet kan inte avsättas eller bli föremål för sanktioner för att ha utfört sina arbetsuppgifter.

Dataskyddsbudet är bunden av sekretess inom ramen för sitt uppdrag i enlighet med gällande lagstiftning.



8 GDPR-samordnare

8.1 Utnämning av GDPR-samordnare

Kanslichef är kommunövergripande GDPR-samordnare tillika den som kommer att koordinera dataskyddsarbete inom kommunen. Minst en GDPR-samordnare utses av respektive förvaltningschef, samordnaren kommer att bli ansvarig för dataskyddsfrågor inom respektive kommunstyrelse/nämnd/kommunalt bolag.

8.2 Kommunövergripande GDPR-samordnarens uppgifter och ansvar

Kommunövergripande GDPR-samordnaren har mandat att leda och koordinera dataskyddsarbete inom kommunen och kommunala bolag och ska:

- Ansvara för att planera dataskyddsarbete på kommunövergripande nivå
- Ta fram rutiner och processer som krävs för att personuppgiftsansvariga ska uppfylla GDPR krav
- Bygga upp en fungerande dataskyddsorganisation
- Hålla regelbunden kontakt med GDPR-samordnare för personuppgiftsansvariga inom kommunen samt samordnare för kommunala bolag
- Organisera och genomföra träffar med GDPR-samordnare
- Fungera som kommunens kontaktlänk till dataskyddsombudet
- Sammankalla och leda nätverksmöten för kommunens GDPR-samordnare
- Hålla regelbunden kontakt med dataskyddsombudet, rapportera om hur dataskyddsarbete går till och efterfråga nödvändiga insatser, som till exempel utbildningar med dataskyddsombud, träffar, rådgivning, biträdande i genomförandet av konsekvensbedömningar
- Fungera som kunskapsstöd till GDPR-samordnare
- Delta i nätverksträffar med övriga samarbetskommuners motsvarighet till kommunövergripande GDPR-samordnare
- Vara stöd vid interna utbildningar om GDPR

8.3 GDPR-samordnarens uppgifter och ansvar

GDPR-samordnare har mandat att leda dataskyddsarbete inom personuppgiftsansvariges verksamhet och ska:

- Kunna besvara frågor kring tillämpningen av GDPR



- Ansvara för att personuppgiftsansvarige har ett uppdaterat register över behandlingar av personuppgifter
- Hantera begäran om registerutdrag, rättelse, radering, invändning, begränsning och dataportabilitet
- Biträda då konsekvensbedömningar genomförs, läs mer i kap. 15.
- Utredda personuppgiftsincidenter, läs mer i kap 16 och ansvara för att personuppgiftsincidenter dokumenteras
- Biträda då personuppgiftsbiträdesavtal upprättas av de medarbetare som är ansvariga för respektive huvudavtal
- Ansvara för att personuppgiftsbiträdesavtalet registreras i ett diariesystem eller på annat sätt hållas ordnat tillsammans med huvudavtalet, läs mer i kap. 6.
- Fungera som personuppgiftsansvariges kontaktlänk till kommunövergripande GDPR-samordnare och dataskyddsombudet

GDPR-samordnaren ska informera dataskyddsombudet om dataskyddsarbetet var tredje månad, eller oftare vid behov. Dataskyddsombudet kan utöver detta begära ytterligare information från GDPR-samordnaren.

GDPR-samordnaren meddelar även dataskyddsombudet om det finns behov av utbildningsinsatser kring GDPR. GDPR-samordnaren kan, i dialog med dataskyddsombudet och sin chef, delta i eller själv genomföra utbildningar kring GDPR.

8.4 Samverkan mellan kommunerna

GDPR-samordnarna inom respektive verksamhetsområde kommunicerar regelbundet med sina motsvarigheter hos de andra kommunerna. Gemensamma möten hålls med syftet att diskutera gemensamma frågor samt dela erfarenheter. Mötena äger rum fyra gånger per år, eller vid behov, och organiseras av dataskyddsombudet och/eller GDPR-samordnare.

9 Personuppgifter

9.1 Vad är en personuppgift?

Personuppgifter är alla uppgifter som avser en identifierad eller identifierbar fysisk person och som direkt eller indirekt kan identifiera en person. Avgörande är att uppgiften enskild eller i kombination med andra uppgifter kan knytas till en levande person. Dataskyddsförordningen omfattar inte avlidna personer. Exempel på personuppgifter är:

- Personnummer
- Namn
- Efternamn
- Telefonnummer
- Adress



- IP-adress
- Foto
- Fastighetsbeteckning
- Kontonummer
- Videoupptagning
- Ljudinspelningar

9.2 Känsliga personuppgifter

Vissa personuppgifter är till sin natur särskilt känsliga och har därför ett starkare skydd. De kallas för känsliga personuppgifter. Det är som huvudregel förbjudet att behandla känsliga personuppgifter, men det finns undantag. Se till exempel tillsynsmyndighetens hemsida och de författningar som det hänvisas till i BILAGA 2. Innan man behandlar känsliga personuppgifter måste man ha klart för sig vilket stöd man har för behandlingen.

Känsliga personuppgifter är uppgifter om:

- Ras och etniskt ursprung.
- Politiska åsikter.
- Religiös eller filosofisk övertygelse. Att någon inte tillhör någon religion alls är också en känslig personuppgift.
- Medlemskap i fackförening.
- Hälsa, vilket omfattar alla aspekter av en persons hälsa, till exempel uppgifter om sjukdom eller funktionshinder.
- Genetiska uppgifter, vilket är uppgifter som ger information om en persons nedärva eller förvärvade genetiska kännetecken. Genetiska uppgifter kan till exempel framgå av en dna-analys.
- Biometriska uppgifter, vilket är uppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga egenskaper och gör det möjligt att identifiera människor, till exempel genom fingeravtrycksavläsning eller ögonskanning.
- Sexualliv eller sexuell läggning.

9.3 Personnummer och samordningsnummer, andra extra skyddsvärda personuppgifter

Personnummer och samordningsnummer är inte känsliga personuppgifter enligt dataskyddsförordningen. Däremot är personnummer och samordningsnummer extra skyddsvärda och måste därför behandlas extra försiktigt. 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.



Det finns även andra personuppgifter som kräver att vidta extra säkerhetsåtgärder med hänsyn tagen till uppgifternas art och risken som behandlingen medför för den registrerade (artikel 32 GDPR). Dessa uppgifter omnämns ofta som *integritetskänsliga personuppgifter*, men uttrycken *extra skyddsvärda personuppgifter* eller *särskild skyddsvärda personuppgifter* är också vanligt förekommande. På känslighetsskala ligger dessa mellan helt harmlösa uppgifter och känsliga uppgifter.

Exempel på extra skyddsvärda personuppgifter är:

- Personnummer
- Samordningsnummer
- Uppgifter om skyddade personer
- Uppgifter om ekonomisk situation
- Uppgifter om civiltillstånd
- Uppgifter om brott eller misstanke om brott
- Uppgifter om social situation
- Information om omfattas av sekretess/tystnadsplikt
- Inkomst
- Skulder
- Omdömen och bedömningar
- Prestationsmätningar



10. Behandling av personuppgifter

10.1 Vad är en behandling?

Dataskyddsförordningen gäller för helt eller delvis automatiserad behandling av personuppgifter. Alla former av åtgärder med personuppgifter, oberoende av om de utförs automatiserat eller inte, är personuppgiftsbehandling, till exempel:

- 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.

Även personuppgifter i e-post och i dokument på servrar, i en enkel lista, på webbplatser och i annat ostrukturerat material omfattas av dataskyddsförordningen.

Dataskyddsförordningen gäller för helt eller delvis automatiserad (digital) behandling av personuppgifter. Ett exempel på delvis automatiserad behandling är när personuppgifter samlas in manuellt i syfte att senare föras in i ett automatiserat register.

Dataskyddsförordningen gäller också för manuell behandling (pappersform) av personuppgifter om personuppgifterna ingår eller är avsedda att ingå i ett manuellt register som är sökbart enligt särskilda kriterier. Att kriterier står i plural i dataskyddsförordningen har ansetts betyda att det ska finnas mer än två sökvägar, såsom namn och e-postadress. Är registret inte sökbart med hjälp av någon personuppgift omfattas det inte av dataskyddsförordningen.

Exempel: En lärare har för hand upprättat en klasslista med för- och efternamn och adresser till eleverna i klassen. Klasslistan finns tillgänglig i en pärm, som står i klassrummet. Klasslistan är helt manuell, men är sökbar enligt två sökvägar (namn och adress), och sökvägarna i sig utgör personuppgifter. Klasslistan omfattas alltså av dataskyddsförordningen, trots att den aldrig behandlas digitalt.



10.2 Behandling av känsliga personuppgifter

Behandling av känsliga personuppgifter är som huvudregel förbjuden. Det går dock att behandla sådana uppgifter om man har lagstöd och iakttar försiktighet. I avsnitt 9.2 framgår vad som menas med känsliga personuppgifter. För att behandling av känsliga personuppgifter ska vara tillåten krävs ett giltigt undantag från förbudet, se avsnitt 9.2 och bilaga 2.

10.3 Behandling av personnummer och samordningsnummer

Personnummer och samordningsnummer är extra skyddsvärda personuppgifter även om de inte är känsliga personuppgifter enligt dataskyddsförordningen. Man får bara behandla personnummer och samordningsnummer när det är klart motiverat med hänsyn till:

- Ändamålet med behandlingen (personuppgiftsansvariges syfte med att registrera personnummer ska klart motivera behandlingen)
- Vikten av en säker identifiering (behandling av personnummer är nödvändigt för att kunna identifiera de registrerade på ett säkert sätt), eller
- något annat beaktansvärt skäl (det finns något annat som klart motiverar registreringen).

Exempel: Arbetsgivare måste ha information om de anställdas personnummer för att kunna betala ut lön.

10.4 Behandla redan insamlade personuppgifter på ett nytt sätt

Om man vill börja behandla redan insamlade personuppgifter på ett nytt sätt måste det vara förenligt med de ursprungliga ändamålen. I sådana fall kan man stödja sig på samma rättsliga grund som användes när personuppgifterna samlades in (i kapitel 11 finns mer information om rättsliga grunder). De registrerade måste informeras om den nya personuppgiftsbehandlingen innan den påbörjas.

När det bedöms om en ny personuppgiftsbehandling är förenlig med tidigare ändamål ska man bland annat ta hänsyn till och ställa sig följande frågor:

- Vilka kopplingar finns mellan ändamålen med den ursprungliga personuppgiftsbehandlingen och den nya?
- I vilket sammanhang har personuppgifterna samlats in, vilket förhållande har de registrerade till oss som personuppgiftsansvarig och vilken personuppgiftsbehandling kan de registrerade rimligen förvänta sig?
- Vilken typ av personuppgifter behandlas, är uppgifterna känsliga?
- Vilka konsekvenser kan personuppgiftsbehandlingen få för de registrerade?
- Vilka skyddsåtgärder finns, till exempel behörighetsstyrning, kryptering och pseudonymisering?



Det är som regel förenligt med de ursprungliga ändamålen att behandla personuppgifter även för:

- Arkivändamål av allmänt intresse
- Vetenskapliga eller historiska forskningsändamål
- Statistiska ändamål.

Den personuppgiftsansvarige måste dock ha vidtagit lämpliga säkerhetsåtgärder för att skydda de registrerades rättigheter.



11. Rättslig grund för behandling av personuppgifter

11.1 Inledande om rättsliga grunderna och hur de används

En behandling av personuppgifter är endast laglig om det finns en rättslig grund för behandlingen. De rättsliga grunderna för behandlingen framgår av artikel 6 GDPR. Det finns sex rättsliga grunder:

- Myndighetsutövning och uppgift av allmänt intresse
- Rättslig förpliktelse
- Avtal
- Samtycke
- Intresseavvägning
- Grundläggande intresse

Myndigheter och andra inom kommunal och offentlig verksamhet ska främst använda följande grunder:

- Rättslig förpliktelse.
- Uppgift av allmänt intresse eller myndighetsutövning.
- Avtal.

Ibland kan privata företag vara verksamma inom offentlig verksamhet, till exempel när skolor eller hälso- och sjukvård bedrivs i privat regi. De utför då en uppgift av allmänt intresse och ska stödja sig på samma rättsliga grunder som en myndighet. Myndigheter, som till exempel kommuner, får *inte* använda sig av en intresseavvägning när de fullgör sina uppgifter.

11.2 Myndighetsutövning och uppgift av allmänt intresse

Den här rättsliga grunden innebär att personuppgiftsbehandling är tillåten om personuppgiftsansvarig behandlar personuppgifter i myndighetsutövning eller utför uppgifter av allmänt intresse. Myndighetsutövning kännetecknas av beslut eller andra ensidiga åtgärder som ytterst är ett uttryck för samhällets maktbefogenheter i förhållande till medborgarna. Det är till exempel myndighetsutövning när nämnden beslutar om att en medborgare ska få en viss förmån eller rättighet, eller att medborgaren har en viss skyldighet och föreläggs att göra något. Det kan alltså vara beslut som gynnar den enskilde eller beslut som är betungande.

Myndighetsutövning kan också ske i förhållande mellan myndigheter, till exempel när en myndighet har tillsyn över en annan myndighets verksamhet. Personuppgiftsbehandlingen måste vara nödvändig - Syftet med personuppgiftsbehandlingen måste vara nödvändigt som ett led i nämndens myndighetsutövning. Ändamålet med behandlingen behöver inte, till skillnad från behandling som grundas på rättslig förpliktelse, framgå av den lag där befogenheten att utöva myndighet fastställs. Det räcker med att det finns ett samband mellan ändamålet med behandlingen och myndighetsutövningen.



Utanför begreppet myndighetsutövning faller sådan faktisk verksamhet personuppgiftsansvarige bedriver, som inte innebär tvång. Exempel på sådan verksamhet är när en kommun lämnar upplysningar och råd eller sopar gatorna.

11.3 Rättslig förpliktelse

Den rättsliga grunden rättslig förpliktelse innebär att det finns lagar eller regler som gör att vissa personuppgifter måste behandlas i en verksamhet. Personuppgiftsansvarig får behandla personuppgifter om det är nödvändigt för att uppfylla en rättslig förpliktelse enligt EU-rätt eller svensk rätt, inklusive kollektivavtal. Den som har ansvar för behandlingen (nämnden) ska vara ålagd att uppfylla den rättsliga förpliktelsen.

Det måste vara möjligt för såväl personuppgiftsansvarig som för den registrerade att förstå varför behandlingen av personuppgifter behövs. Det kan exempelvis finnas en lag som anger att personuppgiftsansvarig i en viss situation är skyldiga att lämna uppgifter till en annan myndighet eller en domstol.

Exempel: En arbetsgivare kan utrusta sina bilar med speciell gps-utrustning som används för elektroniska körjournaler för att förenkla redovisningen till Skatteverket.

Arbetsgivaren får dock inte använda uppgifterna som gps:en samlar in för att till exempel kontrollera hur långa raster de anställda tar, utan får enbart spara just de uppgifter Skatteverket kräver.

Här följer några fler situationer med olika typer av rättsliga skyldigheter eller förpliktelser:

- *Att inom hälso- och sjukvården föra journaler.*
- *Arbetsgivare är skyldiga att redovisa skatter och sociala avgifter beträffande arbetstagarna.*
- *Turordningsreglerna vid uppsägning på grund av arbetsbrist gör att arbetsgivaren måste upprätta listor över anställda och lämna dem till facket.*

11.4 Avtal

Den rättsliga grunden avtal innebär att den registrerade har ett avtal eller ska ingå ett avtal med den personuppgiftsansvarige. Det krävs att personuppgiftsbehandlingen är nödvändig, antingen för att fullgöra avtalet med den registrerade eller för att vidta åtgärder på begäran av den registrerade innan avtalet ingås. Den här grunden gäller bara för avtal i där den registrerade är eller avser att bli part.



Exempel 1: Som arbetsgivare får personuppgiftsansvarige behandla personuppgifter om en anställd för att kunna uppfylla anställningsavtalet, till exempel för löneberäkning, registrering av sjukfrånvaro eller i ett flexitidssystem.

Observera att en personuppgiftsansvarig kan behöva vidta åtgärder på begäran av den registrerade innan ett avtal ingås, exempelvis när det behöver kontrolleras om den registrerade har nödvändiga tillstånd.

11.5 Samtycke

Den rättsliga grunden samtycke innebär att den registrerade har sagt ja till personuppgiftsbehandlingen. Samtycke är dock ofta en olämplig rättslig grund för myndigheter, eftersom samtycket måste vara frivilligt och jämlikt. Överväg därför alltid om ni kan använda någon av de andra rättsliga grunderna.

Den som arbetar för en personuppgiftsansvarig nämnd inom en kommun bör tänka på följande när det gäller samtycke:

- **Samtycke är inte första valet.** Om man kan stödja personuppgiftsbehandlingen på någon av de andra fem rättsliga grunderna, så får man inte dessutom inhämta samtycke. Kom ihåg att det ofta är olämpligt att använda sig av samtycke som myndighet.
- **Fråga bara efter samtycke om ni kan respektera ett nej.** Den registrerade ska kunna avgöra om personuppgifterna ska få behandlas, och hen ska alltid kunna säga nej. Maktförhållandet måste dessutom vara jämlikt.
- **Jämlika maktförhållanden.** För att ni ska kunna använda samtycke som rättslig grund måste maktförhållandet vara jämlikt. Tänk på att maktförhållandet ofta är ojämlikt i relationen mellan myndighet och medborgare, och mellan arbetsgivare och arbetstagare. Om det råder ett ojämlikt maktförhållande kan ni inte stödja er på samtycke.
- **Samtycket ska vara frivilligt.** Med frivilligt menas att den registrerade har ett genuint fritt val och kontroll över sina personuppgifter. Samtycket blir därför ogiltigt om någon har utsatts för påverkan. Den registrerade får inte heller drabbas av negativa konsekvenser om hen inte lämnar sitt samtycke.
- **Den registrerade ska kunna ångra sig.** Förklara klart och tydligt för den som ska lämna sitt samtycke att hen alltid har rätt att ångra sig. Det ska vara lika lätt att lämna ett samtycke som att återkalla det. Detta är särskilt viktigt när det gäller barn. **Obs!** Om det är svårt att återkalla samtycket är det inte giltigt. Om den registrerade inte kan eller får återkalla sitt samtycke utan att drabbas av negativa konsekvenser är samtycket inte frivilligt.
- **Den registrerade ska godkänna att personuppgifterna används.** Det ska tydligt framgå att den registrerade godkänner att personuppgifterna används. Samtycket kan



ges genom ett uttalande eller en entydigt bekräftande handling, till exempel med en kryssruta på en webbplats. **Obs!** Förifyllda kryssrutor är inte tillåtna.

- **Eftersom barn enligt dataskyddsförordningen förtjänar särskilt skydd** måste all information som riktar sig till barn vara skriven på ett tydligt och enkelt sätt som barn förstår. Tidigare gällde Datainspektionens tumregel att barn under 15 år generellt inte har tillräcklig mognad för att ge ett giltigt samtycke, men informationen måste alltid bedömas från fall till fall med utgångspunkt i den enskilda individens mognad och förmåga.
- **Barn och ungdomar som inte själva kan tillgodogöra sig informationen** kan inte lämna ett rättsligt giltigt samtycke. I sådana fall ska samtycket istället inhämtas från den som har föräldraansvaret för barnet.

Personuppgiftsansvarig ansvarar också för att ett giltigt samtycke har inhämtas och behöver kunna visa både att den registrerade har fått relevant information och att vårt arbetssätt uppfyller kraven. Det är därför viktigt att dokumentera:

- Hur samtycket inhämtades
- när samtycket inhämtades samt
- vilken information den registrerade fått.

Exempel på när samtycke kan användas och exempel på när samtycke inte får användas finns på datainspektionens hemsida.

Exempel 1: En nämnd planerar vägarbeten. Nämnden erbjuder invånarna möjlighet att anmäla sig för att få uppdateringar via e-post. Nämnden är tydlig med att det är frivilligt att anmäla sig och inhämtar samtycke för att använda e-postadresserna för endast detta ändamål. Invånare som inte vill delta har inte gått miste om någon grundläggande service från myndigheten. Informationen finns även publikt på kommunens webbplats.

Exempel 2: Arbetsgivaren vill filma på delar av kontoret. Arbetsgivaren frågar alla medarbetare som sitter på den berörda delen av kontoret efter deras samtycke, eftersom de kan synas i bakgrunden på filmen. De som inte vill bli filmade ska inte drabbas av några negativa konsekvenser, utan får istället likvärdiga arbetsplatser någon annanstans i byggnaden under den tid filminspelningen pågår.

Exempel när samtycke INTE kan användas: En medborgare ansöker om en biståndsinsats. För att vi ska kunna hantera ansökan och komma fram till ett beslut så måste vi behandla medborgarens personuppgifter. Vi agerar här som myndighet gentemot medborgaren och maktförhållandet mellan oss är väldigt ojämnt. Samtycket skulle också kunna upplevas som villkorat – om du inte samtycker så får du inget bistånd. Samtycke kan inte användas som rättslig grund för behandlingen. Rätt grund är istället myndighetsutövning.



11.6 Grundläggande intresse

Den här rättsliga grunden innebär att personuppgifter får behandlas om det är nödvändigt för att rädda liv. Det är väldigt få verksamheter som kommer att hänvisa till den här rättsliga grunden. I första hand är den aktuell inom vården.

Personuppgiftsansvarige får behandla personuppgifter om det är nödvändigt för att rädda den registrerades eller någon annan persons liv. Det kallas att skydda intressen som är av grundläggande betydelse. I huvudsak handlar det om tillfällen när den registrerade inte kan fatta beslut eller lämna samtycke, till exempel om en person är medvetslös.

Exempel: En person har plötsligt blivit sjuk och förlorat medvetandet. Vård och räddningstjänst får behandla personuppgifter för att kontrollera blodgrupp och sjukdomshistoria och för att kontakta anhöriga. Anställd inom till exempel hemtjänst eller skola får också lämna personuppgifter till vård och räddningstjänst. Arbetsgivare får också lämna vidare anställds personuppgifter i den situationen etc.

Den här rättsliga grunden kan vi bara använda i mycket begränsad omfattning.

Om det går att lösa situationen på ett annat sätt, gör det. Det kanske till och med går att undvika att behandla personuppgifterna.

Den här situationen uppstår inte om vården är planerad. Då behandlar vårdgivaren patientens personuppgifter med en annan rättslig grund, nämligen uppgift av allmänt intresse. Om en person själv är kapabel att fatta egna beslut och inte samtycker till behandlingen får vi inte behandla personens personuppgifter med denna rättsliga grund.

Personuppgiftsbehandlingen måste vara nödvändig - Det måste vara nödvändigt att behandla personuppgifterna för att vi ska kunna hänvisa till den här rättsliga grunden. Om vi kan ta tillvara den registrerades rättigheter på något annat mindre påträngande sätt kan vi inte hänvisa till att vi skyddar grundläggande intressen. Det kanske till exempel går att behandla en patient utan personuppgifterna. Om det går att lösa på ett annat sätt – gör det. Behandla personuppgifter med den här rättsliga grunden bara om det inte uppenbart finns en annan rättslig grund. I vissa fall kanske det är möjligt att ta tillvara en persons grundläggande intressen med stöd av den rättsliga grunden allmänt intresse.



12. Den registrerades rättigheter

Dataskyddsförordningen ger de registrerade ett flertal rättigheter vad gäller behandling av personuppgifter. Det är personuppgiftsansvariges ansvar se till att tillräckliga processer finns för att tillmötesgå de registrerade så att de kan tillgodose sina rättigheter. Den grundläggande regleringen om rättigheterna finns i artikel 12-20 GDPR.

De registrerade har följande rättigheter:

- Rätt till information
- Rätt till rättelse
- Rätt till radering (rätten att bli bortglömd)
- Rätt till begränsning av behandling
- Rätt till dataportabilitet
- Rätt att inte bli föremål för automatiserat beslutsfattande eller inbegripet profilering
- Rätt att lämna klagomål
- Rätt att begära skadestånd

12.1 Rätt till information

Den registrerade har rätt att få information när hans eller hennes personuppgifter behandlas. Information om personuppgiftsbehandlingen ska lämnas av den personuppgiftsansvarige både när uppgifterna samlas in och när den registrerade annars begär det. Därutöver finns det vissa tillfällen när särskild information ska ges till den registrerade, till exempel om det inträffar ett dataintrång eller liknande (en personuppgiftsincident) hos den personuppgiftsansvarige och det finns risk för till exempel identitetsstöld eller bedrägeri.

Informationen ska tillhandahållas den registrerade kostnadsfritt i en lättillgänglig, skriftlig form (vilket kan vara i elektronisk form) och med ett tydligt och enkelt språk. I dataskyddsförordningen anges utförligt vilken information som ska ges. Bland annat ska information lämnas om kontaktuppgifter till den personuppgiftsansvarige, den rättsliga grunden för behandlingen och ändamålet med behandlingen.

Information om en specifik behandling av personuppgifter ska alltid ges till den registrerade innan behandlingen påbörjas. Inhämtas personuppgifterna från den registrerade själv lämnas information lämpligast i samband med insamlandet. Inhämtas personuppgifterna från någon annan part, ska den personuppgiftsansvarige lämna information i samband med att personuppgifterna första gången registreras.

Information behöver inte lämnas om det finns andra bestämmelser som gäller framför dataskyddsförordningen, t.ex. om vissa uppgifter omfattas av sekretess. Information behöver inte lämnas om sådant som den registrerade redan känner till, eller om det är omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.



Informationen ska omfatta uppgift om den personuppgiftsansvariges identitet, dvs. kommunens adress, nämnd och kontaktperson, uppgift om ändamålen med behandlingen och all övrig information som behövs för att den registrerade ska kunna ta till vara sina rättigheter i samband med behandlingen, såsom information om mottagarna av uppgifterna, skyldighet att lämna uppgift och rätten att ansöka om information och få rättelse. Den registrerade ska om möjligt även få kännedom om hur länge personuppgifterna finns lagrade.

12.2 Registerutdrag

Den registrerade har rätt att få information om personuppgifter som rör honom eller henne behandlas, Vid en begäran om registerutdrag ska personuppgiftsansvarige lämna följande information:

- Vilka uppgifter om sökande som behandlas.
- Varifrån dessa uppgifter har hämtats.
- Ändamålen med behandlingen.
- Till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut.
- Eventuell överföring till tredje land, och i så fall vilka skyddsåtgärder som har vidtagits.
- Hur länge verksamheten sparar uppgifterna.
- Förekomsten av automatiserat beslutsfattande och vilka följderna blir för den registrerade.
- Personuppgiftsansvarige ska även informera den registrerade om rätten att lämna klagomål till tillsynsmyndigheten, rätten att bli raderad, samt rätten att invända mot och begära begränsning av en personuppgiftsbehandling.

Den sökande har rätt att få ett skriftligt besked inom en månad från att ansökan inkom. Om beskedet tar längre tid, ska den sökande underrättas om detta innan en månad har passerat.

12.3 Rättelse

Varje person har rätt att vända sig till ett företag eller myndighet som behandlar personuppgifter och be att få felaktiga uppgifter rättade. Det innebär också att den enskilde har rätt att komplettera med sådana personuppgifter som saknas och som är relevanta med hänsyn till ändamålet med personuppgiftsbehandlingen. Att den som behandlar personuppgifter också själv måste se till att uppgifterna är korrekta och uppdaterade framgår redan av de grundläggande principerna i dataskyddsförordningen.

Om uppgifter rättas på den enskildes begäran måste företaget eller myndigheten också informera dem som de har lämnat ut uppgifter till om att uppgifter rättats. Det gäller dock inte om det skulle visa sig omöjligt eller innebära en alltför betungande insats. Den enskilde har också rätt att begära att få information om till vem uppgifter har lämnats ut.



Rättelse ska göras utan onödigt dröjsmål om den personuppgiftsansvarige har felaktiga personuppgifter som rör den registrerade. Med beaktande av ändamålet med behandlingen, ska den registrerade ha rätt att komplettera ofullständiga personuppgifter, bland annat genom att tillhandahålla ett kompletterande utlåtande.

12.4 Radering

Varje person har rätt att vända sig till ett företag eller en myndighet som behandlar personuppgifter och be att uppgifterna som avser honom eller henne raderas. Uppgifterna måste raderas i följande fall:

- Om uppgifterna inte längre behövs för de ändamål som de samlades in för
- Om behandlingen grundar sig på den enskildes samtycke och denne återkallar samtycket
- Om behandlingen sker för direktmarknadsföring och den enskilde motsätter sig att uppgifterna behandlas
- Om den enskilde motsätter sig personuppgiftsbehandling som sker inom ramen för myndighetsutövning eller efter en intresseavvägning och det inte finns berättigade skäl som väger tyngre än den enskildes intresse
- Om personuppgifterna har behandlats olagligt
- Om radering krävs för att uppfylla en rättslig skyldighet
- Om personuppgifterna avser barn och har samlats in i samband med att barnet skapar en profil i ett socialt nätverk

Om uppgifter raderas på den enskildes begäran måste företaget eller myndigheten också informera dem som de har lämnat ut uppgifter till om raderingen. Det gäller dock inte om det skulle visa sig omöjligt eller innebär en alltför betungande insats. Den enskilde har också rätt att begära att få information om till vem uppgifter har lämnats ut.

När personuppgifterna har publicerats eller på annat sätt gjorts offentliga (i ett socialt nätverk, ett internetforum eller på en webbsida) räcker det inte alltid att de raderas där. I dessa situationer ska den som offentliggjort uppgifterna också vidta rimliga åtgärder för att informera andra som behandlar uppgifterna om den enskildes begäran så att även kopior av eller länkar till uppgifterna tas bort.

Det finns undantag från rätten till radering och skyldigheten att informera andra om det är nödvändigt för att tillgodose andra viktiga rättigheter. Personuppgifterna ska inte raderas om behandlingen är nödvändig av följande skäl:

- För att utöva rätten till yttrande- och informationsfrihet
- 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
- För skäl som rör ett viktigt allmänt intresse på folkhälsoområdet enligt artikel 9.2 h och i samt artikel 9.3



- 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
- För att kunna fastställa, göra gällande eller försvara rättsliga anspråk

12.5 Begränsning av behandling

Enskilda har i vissa fall rätt att kräva att behandlingen av personuppgifter begränsas. Med begränsning menas att uppgifterna markeras så att dessa i framtiden endast får behandlas för vissa avgränsade syften.

Rätten till begränsning gäller bland annat när den registrerade anser att uppgifterna är felaktiga och begär rättelse. I sådana fall kan den registrerade även begära att behandlingen av uppgifterna begränsas under tiden uppgifternas korrekthet utreds. När begränsningen upphör ska den enskilde informeras om detta.

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

- a) Den registrerade bestrider personuppgifternas korrekthet, under en tid som ger den personuppgiftsansvarige en möjlighet att kontrollera om personuppgifterna är korrekta.
- b) Behandlingen är olaglig och den registrerade motsätter sig att personuppgifterna raderas och i stället begär en begränsning av deras användning.
- c) Den personuppgiftsansvarige behöver inte längre personuppgifterna för ändamålen med behandlingen men den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.
- d) Den registrerade har invänt mot behandling i enlighet med artikel 21.1 i väntan på kontroll av huruvida den personuppgiftsansvariges berättigade skäl väger tyngre än den registrerades berättigade skäl.

Om behandlingen har begränsats i enlighet med punkt a 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.

12.6 Rätt till dataportabilitet (överföring)

Den som har lämnat sina personuppgifter har i vissa fall rätt att få ut och använda sina personuppgifter på annat håll till exempel i en annan social medietjänst (rätten till dataportabilitet). Den som har tagit emot personuppgifterna är skyldig att underlätta en sådan överflyttning av personuppgifter. *En förutsättning är att den personuppgiftsansvarige behandlar personuppgifter med stöd av ett samtycke från den registrerade eller för att*



uppfylla ett avtal med den registrerade och det gäller bara sådana personuppgifter som den registrerade själv har lämnat. Rätten till dataportabilitet är en nyhet i dataskyddsförordningen.

12.7 Rätt att göra invändningar

En enskild har i vissa fall rätt att invända mot den personuppgiftsansvariges behandling av hans eller hennes personuppgifter. Rätten att invända gäller när personuppgifter behandlas för att utföra en uppgift av allmänt intresse, som ett led i myndighetsutövning eller efter en intresseavvägning. Om den enskilde invänder mot behandlingen får den personuppgiftsansvarige endast fortsätta att behandla uppgifterna om det går att visa att det finns tvingande berättigade skäl till att uppgifterna måste behandlas som väger tyngre än den enskildes intressen, rättigheter och friheter eller om behandlingen sker för fastställande, utövande eller försvar av rättsliga anspråk.

Den enskilde har alltid rätt att invända mot att hans eller hennes personuppgifter används för direkt marknadsföring. En sådan invändning kan göras när som helst. Görs en invändning mot direkt marknadsföring, får personuppgifterna inte längre behandlas för sådana ändamål. Särskilda regler gäller för personuppgifter som behandlas för vetenskapliga och historiska forskningsändamål eller statistiska ändamål.

Den personuppgiftsansvarige måste informera de registrerade om rätten att göra invändningar.

12.8 Automatiserat beslutsfattande eller profilering

Den enskilde har rätt att inte bli föremål för ett beslut som enbart grundas på någon form av automatiserat beslutsfattande, inbegripet profilering, om beslutet kan ha rättsliga följder för den enskilde eller på liknande sätt i betydande grad påverkar honom eller henne.

Automatiserat beslutsfattande kan till exempel vara ett automatiserat avslag på en kreditansökan på internet eller vid ett nekande besked från e-rekrytering via internet utan personlig kontakt.

Automatiserat beslutsfattande kan vara tillåtet om det är nödvändigt för ingående eller fullgörande av ett avtal mellan den registrerade och den personuppgiftsansvarige eller om den enskilde har gett sitt uttryckliga samtycke. Det kan även vara tillåtet enligt särskild lagstiftning. Den personuppgiftsansvarige måste informera de registrerade om att automatiserat beslutsfattande används enligt den generella informationsskyldigheten i förordningen.

Automatiserade beslut kan fattas med eller utan profilering. Omvänt kan profilering användas utan att det leder till ett automatiserat beslut. Profilering innebär varje form av automatisk behandling av personuppgifter då uppgifterna används för att bedöma vissa personliga egenskaper, i synnerhet för att analysera eller förutsäga personens arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar.



Profilering utgör en behandling av personuppgifter som måste utföras i enlighet med samtliga bestämmelser i dataskyddsförordningen.

12.9 Avgift

Utgångspunkten är att information som lämnas och åtgärder som vidtas enligt artiklarna 13-22 och 34 ska tillgodoses utan att avgift tas ut från den registrerade. Personuppgiftsansvarig *kan* begära att avgift ska tas ut i samband med repetitiv och uppenbart ogrundad begäran om att lämna ut. Det förutsätter att respektive kommun beslutar om och hur sådan avgift i så fall ska tas ut.

12.10 Beslut och överklagande

Beslut som fattats i anledning av den registrerades rättigheter som beskrivs i artiklarna 12.5 och 15-21 dataskyddsförordningen kan överklagas till allmän förvaltningsdomstol, detsamma gäller eventuella beslut att ta ut avgift. Att beslut ska fattas och att de kan överklagas framgår av 7 kap 2 § dataskyddslagen och förarbeten till den bestämmelsen.

12.11 Klagomål

Den som anser att någon behandlar uppgifter om honom eller henne i strid med dataskyddsförordningen kan lämna in ett klagomål till Datainspektionen. Datainspektionen tar del av alla klagomål och bedömer om tillsyn ska inledas och lämnar därefter besked till den som fört fram klagomålet.

12.12 Skadestånd

En person som har lidit skada på grund av att hans eller hennes personuppgifter har behandlats i strid med dataskyddsförordningen kan ha rätt till skadestånd av den eller de personuppgiftsansvariga som medverkat vid behandlingen.

Ett personuppgiftsbiträde kan också bli skadeståndsansvarigt om denne har brutit mot de bestämmelser som specifikt riktar sig till biträden eller har behandlat uppgifter i strid med den ansvariges instruktioner. Den enskilde kan begära skadestånd från den personuppgiftsansvarige eller personuppgiftsbiträdet eller väcka skadeståndstalan i domstol.

Den som lidit skada har i princip rätt att få ersättning för hela skadan av antingen den personuppgiftsansvarige eller personuppgiftsbiträdet. De får sedan i sin tur reglera detta sinsemellan. En personuppgiftsansvarig eller ett biträde har dock ingen skyldighet att betala ersättning om de kan visa att de inte på något sätt är ansvariga för skadan.



13. Säkerhetsåtgärder, behörighetsstyrning och åtkomst, radering

Personuppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna med användning av tekniska och organisatoriska åtgärder.

Exempel på tekniska åtgärder som måste kontrolleras är:

- Tillräckliga back-up rutiner
- Tillräckliga brandväggar
- Lösenordskyddade trådlösa nätverk
- Uppdaterat virussydd
- Lösenordsskydd för mobila enheter såsom mobiltelefoner och surfplattor
- Skydd mot obehörig intern åtkomst
- Lösenordskrav
- Kryptering vid behov
- Loggning av, åtkomst till och användning av IT-system mm

Organisatoriska säkerhetsåtgärder kan innebära att behörighetskontroll används för de system som innehåller personuppgifter, loggning av åtkomst till personuppgifter eller att datorer och dylikt som innehåller personuppgifter ska förvaras så att obehörig åtkomst försvåras och inte lämnas framme.

Personuppgifter får inte bevaras längre än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Genom att upprätta och följa en gallringsrutin för respektive databas/behandling säkerställer man det strukturerade gallringsarbetet. Även personuppgifter i så kallat ostrukturerat material såsom i dokument på servrar, i en enkel lista, på webbplatser etc. behöver raderas när ändamålet med behandlingen är uppfyllt.



14. Överföring till tredje land

Överföring av personuppgifter till tredje land är när personuppgifter blir tillgängliga för någon i ett land utanför EU/EES-området (så kallad tredjelandsöverföring). Listan med länder som omfattas av dataskyddsförordningen finns i BILAGA 1.

För överföring av personuppgifter till länder utanför EU och EES gäller särskilda regler. Dataskyddsförordningen innebär att alla EU:s medlemsstater samt EES-länderna har ett likvärdigt skydd för personuppgifter och personlig integritet och därför kan personuppgifter föras över fritt inom det området utan begränsningar. För länder utanför det området finns däremot inte några generella regler som ger motsvarande garantier och därför får tredjelandsöverföring endast ske under särskilda förutsättningar. Det här berör varje form av överföring av information över gränserna, t ex många online IT-tjänster, molnbaserade tjänster, tjänster för extern åtkomst eller globala databaser mm och behöver analyseras särskilt.

Exempel på överföring av personuppgifter till tredje land:

- När ett dokument som innehåller personuppgifter skickas till någon i ett land utanför EU/EE via e-post
- När ett personuppgiftbiträde anlitas i ett land utanför EU/EES.
- När någon utanför EU/EES får tillgång, exempelvis läsbehörighet, till personuppgifter som finns lagrade inom EU/EES.
- När personuppgifter lagras i en molntjänst som är baserad utanför EU/EES.
- När personuppgifter lagras, till exempel på en server, i ett land utanför EU/EES.

Att publicera något på internet är *inte* tredjelandsöverföring om webbplatsen lagras hos en internetleverantör som är etablerad inom EU.

14.1 Adekvat skyddsnivå

EU-kommissionen kan fatta beslut om att ett land har en tillräckligt hög skyddsnivå och personuppgiftsansvarig får då föra över personuppgifter dit utan att de förutsättningar som beskrivs nedan i avsnitt 14.2 är uppfyllda. I dataskyddsförordningen kallas det för adekvat skyddsnivå. Det kan även gälla ett visst territorium, en internationell organisation eller en eller flera sektorer i ett tredje land.

När EU-kommissionen fattar beslut om adekvat skyddsnivå tittar de bland annat på landets lagar och internationella åtaganden, vilka möjligheter den registrerade har att få rättslig prövning och om landet respekterar de mänskliga rättigheterna och de grundläggande friheterna. EU-kommissionen kontrollerar också att det finns oberoende tillsynsmyndigheter som ansvarar för att dataskyddsreglerna följs och som kan hjälpa den registrerade.



Till skillnad från i personuppgiftslagen finns det *inte* längre utrymme för den personuppgiftsansvarige att själv avgöra om det finns en adekvat skyddsnivå eller inte. Det är bara EU-kommissionen som kan fatta ett sådant beslut.

EU-kommissionen har fattat beslut om att skyddsnivån i till exempel dessa länder är adekvat, det vill säga tillräckligt hög enligt dataskyddsförordningen:

- Andorra
- Argentina
- Bailiwick of Guernsey
- Färöarna
- Isle of Man
- Israel
- Jersey
- Nya Zeeland
- Schweiz
- Uruguay

Dessutom har EU-kommissionen bedömt att skyddsnivån är adekvat på vissa områden eller under särskilda villkor i till exempel Kanada, om deras lagstiftning för skydd av personuppgifter i privat sektor är tillämplig på mottagarens personuppgiftsbehandling.

Nya beslut fattas löpande, uppgifterna ska kontrolleras hos tillsynsmyndigheten vid behov.

14.2 När får uppgifter annars överföras till tredje land?

Personuppgifter får överföras till ett land utanför EU/EES utan att det finns beslut om att landet har en adekvat skyddsnivå om det finns:

- Bindande företagsbestämmelser
- Standardavtalsklausuler som EU-kommissionen har beslutat
- Godkända uppförandekoder eller certifieringsmekanismer
- Rättsligt bindande instrument mellan myndigheter
- Tillstånd från tillsynsmyndigheten

Det måste dessutom finnas lagstadgade rättigheter och möjlighet för de registrerade att klaga på personuppgiftsbehandlingen och få den prövad i domstol.

14.1.1 Bindande företagsbestämmelser

Bindande företagsbestämmelser (Binding Corporate Rules, BCR) är regler som en företagskoncern med bolag i flera olika länder kan ta fram för att reglera sin behandling av personuppgifter. Bindande företagsbestämmelser måste godkännas av tillsynsmyndigheten i Sverige eller någon annan tillsynsmyndighet i EU.



I dataskyddsförordningen finns detaljerade bestämmelser om vad bindande företagsbestämmelser ska innehålla och hur det går till när tillsynsmyndigheten behandlar ärenden om att få bindande företagsbestämmelser godkända. Innan en tillsynsmyndighet godkänner bindande företagsbestämmelser ska den begära yttrande från den Europeiska dataskyddsstyrelsen, där företrädare för alla EU/EES-länders tillsynsmyndigheter är med.

14.1.2 Standardavtalsklausuler som EU-kommissionen har beslutat om
EU-kommissionen har godkänt vissa standardavtalsklausuler som handlar om dataskydd (Standard Contractual Clauses, SCC). Om ni ingår avtal, som innehåller dessa standardavtalsklausuler, med någon utanför EU/EES, så är det tillåtet att överföra personuppgifter till dem. Observera dock att ni inte får ändra i klausulerna. Om det är nödvändigt kan ni få lägga till klausuler om affärsrelaterade frågor, men sådana får då inte strida mot någon standardavtalsklausul.

Standardavtalsklausulerna innehåller skyldigheter dels för personuppgiftsansvariga som vill föra över personuppgifter till länder utanför EU/EES, dels för personuppgiftsansvariga eller personuppgiftsbiträden 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.

Det finns tre alternativ att välja mellan när det gäller standardavtalsklausuler. Alla tre har godkänts av EU-kommissionen. Två av dessa gäller överföring till andra personuppgiftsansvariga i länder utanför EU/EES. Det tredje avser överföring av personuppgifter till personuppgiftsbiträden i länder utanför EU/EES.

De svenska versionerna:

[Alternativ 1](#)

[Alternativ 2](#)

[Alternativ 3](#)

14.1.3 Uppförandekoder och certifieringsmekanismer

Om personuppgiftsansvarig ansluter er till en godkänd uppförandekod eller godkänd certifieringsmekanism kan det vara tillåtet att överföra personuppgifter till länder utanför EU/EES. Detta gäller under förutsättning att dessa medför rättsligt bindande och verkställbara skyldigheter även för mottagaren av personuppgifterna.

14.1.4 Rättsligt bindande instrument mellan myndigheter

Det är tillåtet att grunda en överföring av personuppgifter till ett land utanför EU/EES på ett så kallat rättsligt bindande och verkställbart instrument, om överföringen sker mellan myndigheter. Ett sådant instrument mellan myndigheter kan vara ett samförståndsavtal eller ett informationsutbytesavtal inom till exempel skatteområdet.



14.1.5 Tillstånd från tillsynsmyndigheten

Myndigheter får också överföra personuppgifter till ett land utanför EU/EES om de har fått tillstånd från tillsynsmyndigheten. Ett sådant tillstånd kan lämnas om överföringen grundar sig på avtalsklausuler mellan den som för över personuppgifter och mottagaren av dessa. Om det gäller överföring av personuppgifter mellan myndigheter kan tillstånd även lämnas om överföringen grundar sig på bestämmelser i administrativa överenskommelser som innehåller verkställbara och faktiska rättigheter för de registrerade. Innan tillsynsmyndigheten beslutar om särskilt tillstånd ska ett yttrande inhämtas från den Europeiska dataskyddsstyrelsen, där företrädare för alla EU/EES-länders tillsynsmyndigheter är med.



15. Konsekvensbedömning

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 (artikel 35 dataskyddsförordningen). Artikel 29 gruppen har antagit riktlinjer för hur konsekvensbedömningen ska göras.

Personuppgiftsansvarig, ska påbörja konsekvensbedömningen så tidigt som möjligt och börja även om vissa delar av behandlingen fortfarande är okända. Även personuppgiftsbehandlings som har påbörjats innan dataskyddsförordningen började gälla, omfattas av kravet att en konsekvensbedömning ska genomföras vid behov.

Den personuppgiftsansvarige ska rådfråga dataskyddsombudet om konsekvensbedömningen. Dataskyddsombudet bör även övervaka genomförandet av konsekvensbedömningen. Det är dock alltid den personuppgiftsansvarige som är ansvarig för att konsekvensbedömningen utförs. Konsekvensbedömningen kan utföras av någon annan, inom eller utanför organisationen, men den personuppgiftsansvarige har det yttersta ansvaret. Dataskyddsombudets råd och de beslut som den personuppgiftsansvarige fattar bör dokumenteras i konsekvensbedömningen.

15.1 Prövningen av om konsekvensbedömning ska göras

En konsekvensbedömning ska göras om en viss personuppgiftsbehandling "sannolikt leder till en hög risk för fysiska personers rättigheter och friheter". Riskerna ska i första hand bedömas utifrån dataskydd och integritet, men även utifrån andra grundläggande rättigheter som yttrandefrihet, tankefrihet, fri rörlighet, förbud mot diskriminering, rätt till frihet, samvete och religion. Det krävs en konsekvensbedömning om en behandling sannolikt leder till hög risk för fysiska personers rättigheter och friheter (artikel 35 punkt 1 dataskyddsförordningen).

15.2.1 När ska en konsekvensbedömning göras?

Enligt artikel 35.3 ska en bedömning *särskilt* krävas vid:

1. En systematisk och omfattande bedömning av fysiska personers personliga förhållanden 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.
2. Behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1, eller av personuppgifter som rör fällande domar i brottmål och överträdelse som avses i artikel 10.
3. Systematisk övervakning av en allmän plats i stor omfattning.



Om behandlingen inte ingår i de tre kategorier som framgår av artikel 35.3, ska man göra en bedömning för att komma fram till om en behandling ”sannolikt leder till en hög risk” och om det behövs därför en konsekvensbedömning. Artikel 29 gruppen har sammanställt nio steg, som bedömningen ska göras i.

1. Utvärdering eller poängsättning, som inbegriper profilering och förutsägelse, särskilt ”aspekter avseende den registrerades arbetsprestation, ekonomiska situation, hälsa, personliga preferenser eller intressen, pålitlighet eller beteende, vistelseort eller förflyttningar” (skälen 71 och 91). Exempel på detta kan innefatta finansinstitut som granskar sina kunder mot en databas för kreditupplysning eller mot en databas för bekämpning av penningtvätt och finansiering av terrorism, eller ett bioteknikföretag som erbjuder genetiska tester direkt till konsumenter för att bedöma och förutse risker för sjukdomar/hälsorisker, eller ett företag som utvecklar profiler för beteende eller marknadsföring som grundas på användning av eller navigering på dess webbplats.

2. Automatiskt beslutsfattande med rättsliga eller liknande betydande följder: behandling som har i syfte att fatta beslut om registrerade som har ”rättsliga följder för fysiska personer” eller ”på liknande sätt i betydande grad påverkar fysiska personer” (artikel 35.3 a). Till exempel kan behandlingen leda till utestängning eller diskriminering av enskilda. Behandling som har liten eller ingen påverkan på enskilda uppfyller inte detta särskilda kriterium. Ytterligare förklaringar om dessa begrepp kommer att tillhandahållas i arbetsgruppens kommande riktlinjer om profilering.

3. Systematisk övervakning: behandling som används för att observera, övervaka eller kontrollera registrerade, inbegripet uppgifter som har samlats in genom nätverk eller ”systematisk övervakning av en allmän plats” (artikel 35.3 c)¹⁵. Denna typ av övervakning är ett kriterium eftersom personuppgifter kan samlas in i situationer där de registrerade kanske inte är medvetna om vem som samlar in deras uppgifter eller hur de kommer att användas. Dessutom kan det vara omöjligt för enskilda att undvika att bli föremål för sådan behandling på allmän plats (eller allmänt tillgängliga platser).

4. Känsliga uppgifter eller uppgifter av mycket personlig karaktär: detta omfattar särskilda kategorier av personuppgifter såsom de definieras i artikel 9 (till exempel information om enskildas politiska åsikter) liksom personuppgifter som gäller fällande domar i brottmål och brott såsom de definieras i artikel 10. Ett exempel kan vara ett allmänt sjukhus som lagrar patienternas journaler eller en privatdetektiv som sparar uppgifter om gärningsmän.

Utöver dessa bestämmelser i förordningen kan vissa kategorier av uppgifter anses öka den eventuella risken för enskildas rättigheter och friheter. Sådana personuppgifter anses vara känsliga (såsom detta begrepp normalt förstås), eftersom de är kopplade till verksamhet som har samband med hushållet och privat verksamhet (såsom elektronisk kommunikation vars konfidentialitet ska skyddas), eller eftersom de påverkar utövandet av en grundläggande rättighet (såsom lokaliseringssuppgifter vars insamling medför att den fria rörligheten ifrågasätts) eller eftersom åsidosättandet av dessa rättigheter entydigt får allvarliga



konsekvenser för den registrerades dagliga liv (såsom finansiella uppgifter som kan användas för betalningsbedrägeri). I detta avseende kan det ha betydelse om uppgifterna redan har offentliggjorts av den registrerade eller av tredje man.

Det faktum att personuppgifterna har offentliggjorts kan beaktas som en faktor vid bedömningen av om uppgifterna förväntades användas vidare för särskilda ändamål. Detta kriterium kan även omfatta uppgifter såsom personliga dokument, e-postmeddelanden, dagböcker, kommentarer från läsplattor som är utrustade med kommentarfunktioner och mycket personlig information i applikationer som registrerar aktiviteter.

5. Uppgifter som behandlas i stor omfattning: I förordningen definieras inte vad som avses med stor omfattning, även om viss vägledning ges i skäl 91. Arbetsgruppen rekommenderar i vart fall att följande faktorer beaktas särskilt vid bedömningen av huruvida behandlingen utförs i stor omfattning¹⁶:

- a. Antalet registrerade som berörs, antingen som ett särskilt antal eller som en andel av den aktuella populationen.
- b. Mängden uppgifter och/eller variationen av hanterade dataelement.
- c. Databehandlingens varaktighet eller beständighet.
- d. Behandlingens geografiska omfattning.

6. Matchande eller kombinerande uppgiftsserier, som till exempel kommer från två eller flera behandlingar av uppgifter som utförs i olika syften och/eller av olika personuppgiftsansvariga på ett sätt som överstiger den registrerades rimliga förväntningar.

7. Uppgifter som rör sårbara registrerade (skäl 75): behandling av denna typ av uppgifter är ett kriterium på grund av en ökad maktobalans mellan de registrerade och den personuppgiftsansvarige, vilket innebär att det kan vara svårt för enskilda att på ett enkelt sätt lämna samtycke eller motsätta sig behandling av sina uppgifter eller utöva sina rättigheter. Sårbara registrerade kan omfatta barn (de kan anses inte vara i stånd att medvetet och med eftertanke motsätta sig eller lämna samtycke till behandling av sina uppgifter), anställda, mer sårbara befolkningsgrupper som behöver socialt skydd (psykiskt sjuka personer, asylsökande, äldre personer, patienter osv.), samt i vart fall situationer där en obalans kan fastställas vad gäller förhållandet mellan den registrerade och den personuppgiftsansvarige.

8. Innovativ användning eller tillämpning av nya tekniska eller organisatoriska lösningar, såsom en kombination av fingeravtryck och ansiktigenkänning för förbättrad fysisk åtkomstkontroll osv. I förordningen klargörs (artikel 35.1 och skälen 89 och 91) att användningen av ny teknik, definierad ”i enlighet med den uppnådda nivån av teknisk kunskap” (skäl 91), kan innebära att det behövs en konsekvensbedömning. Detta beror på att användningen av sådan teknik kan omfatta nya former av insamling och användning av uppgifter, eventuellt med hög risk för enskildas rättigheter och friheter. De personliga och

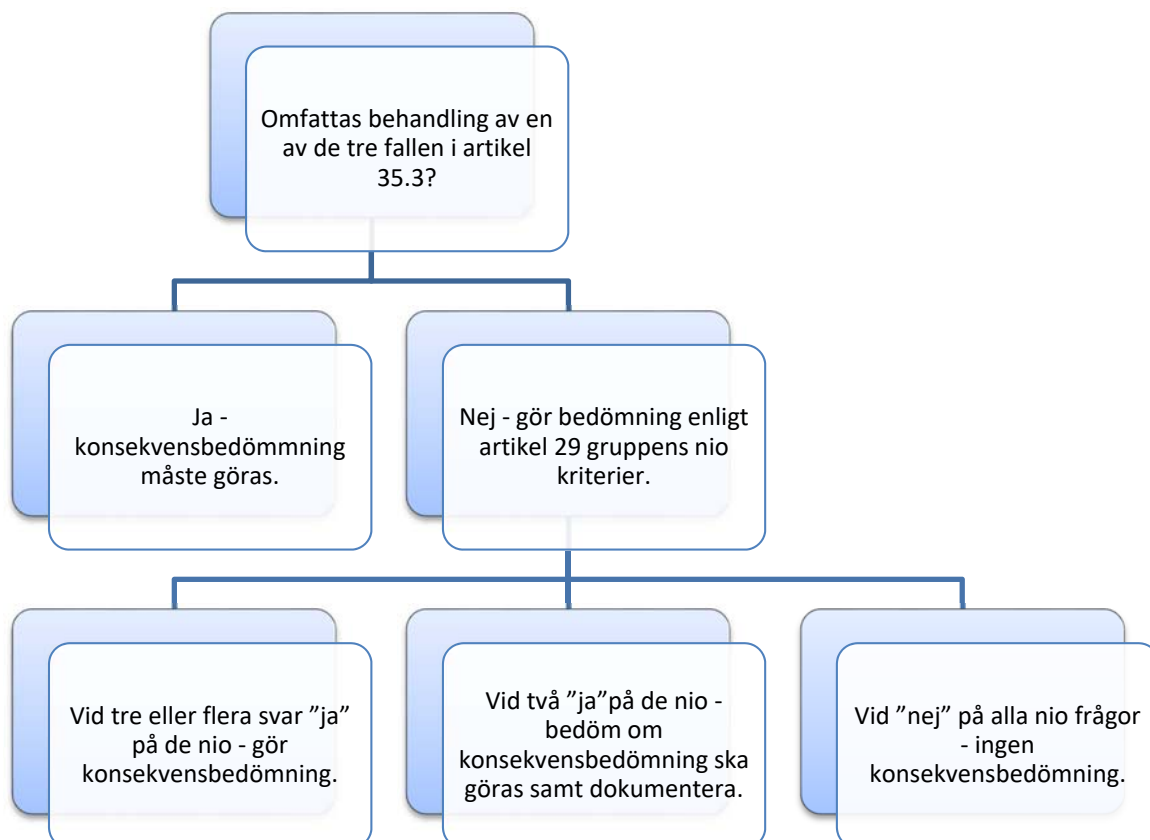


sociala konsekvenserna av användningen av ny teknik kan vara okända. En konsekvensbedömning hjälper den personuppgiftsansvarige att förstå och hantera sådana risker. Till exempel kan vissa ”sakernas internet”-applikationer få betydande konsekvenser för enskildas dagliga liv och integritet och således kräva en konsekvensbedömning.

9. Om behandlingen i sig ”hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal:(artikel 22 och skäl 91). Detta omfattar behandlingar som syftar till att medge, ändra eller neka registrerade tillgång till en tjänst eller att ingå ett avtal. Ett exempel på detta är när en bank granskar sina kunder mot en databas för kreditupplysning för att besluta om de ska erbjudas lån.

I artikel 29-gruppens riktlinjer tilläggs sedan att i de flesta situationer kan en personuppgiftsansvarig anse att en konsekvensbedömning ska utföras om två av dessa kriterier är uppfyllda. Generellt sett anser arbetsgruppen att ju fler kriterier behandlingen uppfyller, desto mer sannolikt är det att det föreligger en hög risk för de registrerades rättigheter och friheter, och att det därför krävs en konsekvensbedömning, oberoende av vilka åtgärder som den personuppgiftsansvarige planerar att vidta. Om man får tre eller flera svar ”ja” på de nio frågorna ska en konsekvensbedömning göras!

Nedan följer en bild som visar de olika stegen vid prövningen.



15.2.2 När ska en konsekvensbedömning inte göras?

Det krävs *inte* en konsekvensbedömning om personuppgiftsbehandlingen:

- Sannolikt *inte* leder till en hög risk för fysiska personers rättigheter och friheter
- Är mycket lik en annan personuppgiftsbehandling där det redan finns en konsekvensbedömning.
- Har sin rättsliga grund i en lag eller förordning, och en konsekvensbedömning redan har genomförts när lagen eller förordningen fastställdes. Datainspektionen känner inte till att det finns några sådana exempel än.

En konsekvensbedömning behöver inte göras om den tilltänkta behandlingen inte innefattar någon av de kriterier som artikel 29 gruppen har tagit fram som bedömningsmall.

15.3 En eller flera behandlingar?

En konsekvensbedömning kan gälla för en eller för flera liknande behandlingar. En enda konsekvensbedömning kan till exempel användas för att bedöma flera behandlingar som liknar varandra vad gäller art, omfattning, innehåll, ändamål och risker, såsom

- Ett antal matvarubutiker ska var och en införa liknande övervakningssystem på likartade platser. De kan göra en enda konsekvensbedömning.
- En organisation vill införa en personuppgiftsbehandling som liknar en annan personuppgiftsbehandling där det redan finns en konsekvensbedömning. Då kan de använda den första bedömningen som referens i sin nya konsekvensbedömning.

Den som gör en gemensam konsekvensbedömning för flera personuppgiftsbehandlingar ska motivera varför en enda konsekvensbedömning har utförts. Motiveringen ska dokumenteras.

15.4 Konsekvensbedömningens innehåll

En konsekvensbedömning ska enligt artikel 29 gruppen innehålla följande:

En systematisk beskrivning av behandlingen

Den systematiska beskrivningen ska innefatta beskrivning av behandlingens art, omfattning, sammanhang och ändamål. Den ska också innehålla beskrivning av vilka personuppgifter som registrerats, vilka mottagare de överförs till och vilken period de kommer att lagras. Det ska finnas en funktionell beskrivning av behandlingen. De tillgångar som är nödvändiga för behandlingen ska beskrivas (maskinvara, programvara, nätverk, personer, papper eller spridningskanaler för papper). Efterlevnad av eventuella godkända uppförandekoder ska beaktas (artikel 35.8).

Bedömning av behovet av och proportionaliteten hos behandlingen (artikel 35.7 b)

De planerade åtgärderna för att visa att förordningen följs som har fastställts (artikel 35.7 d och skäl 90), ska beskrivas. Det ska visas hur åtgärder som bidrar till att behandlingen är proportionell och nödvändiga på grundval av:

- särskilda, uttryckligt angivna och berättigade ändamål (artikel 5.1 b),



- laglig behandling (artikel 6),
- adekvata, relevanta och inte för omfattande uppgifter (artikel 5.1 c),
- begränsad lagringstid (artikel 5.1 e).

Det ska tas upp vilka åtgärder som stärker de registrerades rättigheter som är tillgängliga med beaktande av:

- Information till den registrerade (artiklarna 12, 13 och 14).
- Rätt till tillgång och till dataportabilitet (artiklarna 15 och 20).
- Rätt till rättelse och radering (artiklarna 16, 17 och 19).
- Rätt att göra invändningar och till begränsning av behandling (artiklarna 18, 19 och 21).
- Förhållandet till personuppgiftsbiträden (artikel 28).
- Skyddsåtgärder som vidtagits för internationella överföringar och det ska beskrivas om förhandssamråd skett (artikel 36).

Hantering av risker för de registrerades rättigheter och friheter (artikel 35.7 c)

Det ska göras en uppskattning av riskens ursprung, art, särdrag och allvar (se skäl 84). Mer specifikt, för varje risk ur de registrerades perspektiv:

1. Beaktande av riskens ursprung (skäl 90).
2. Identifiering av möjliga konsekvenser för de registrerades rättigheter och friheter vid händelser, däribland obehörig åtkomst, oönskad ändring och förlust av uppgifter.
3. Identifiering av hot som kan leda till obehörig åtkomst, oönskad ändring och förlust av uppgifter.
4. Uppskattning av sannolikhetsgrad och allvar (skäl 90).
5. Fastställande av planerade åtgärder för att hantera dessa risker (artikel 35.7 d och skäl 90).

Exempel på risker är obehörig åtkomst, oönskad ändring och att uppgifter försvinner.

Medverkan från berörda parter

Medverkan från berörda parter ska dokumenteras, här märks:

1. Rådfrågan av dataskyddsombudet (artikel 35.2).
2. När så är lämpligt, inhämtning av synpunkter från de registrerade eller deras företrädare (artikel 35.9).

15.5 Inhämta synpunkter från de registrerade?

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. Beroende på hur personuppgiftsbehandlingen är planerad att fungera kan man fråga på olika sätt. I vissa fall är det lämpligt med en enkät till allmänheten, ibland kan det vara bra att råd göra med fackliga företrädare. För en skola kan det vara lämpligt att råd göra med elevernas vårdnadshavare.



Om den personuppgiftsansvarige och de registrerade inte har samma syn på behandlingen, ska det dokumenteras. Det är särskilt viktigt om man väljer att gå vidare med personuppgiftsbehandlingen. Om den personuppgiftsansvarige väljer att inte inhämta synpunkter från de registrerade, ska man dokumentera även det. Kanske är det inte lämpligt för att det skulle äventyra företagets affärsplaner, innebära oproportionerligt mycket arbete vara eller genomförbart av andra skäl.

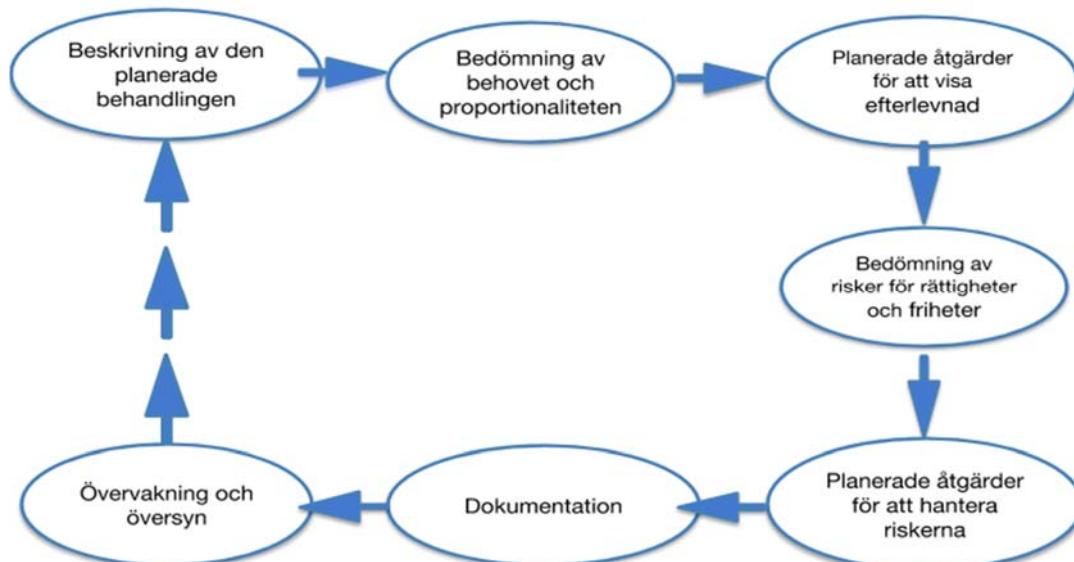
15.6 Ska konsekvensbedömningen offentliggöras?

Det är inte ett rättsligt krav enligt förordningen att offentliggöra en konsekvensbedömning, utan detta är den personuppgiftsansvariges beslut. En upprättad konsekvensbedömning blir dock offentlig hos en kommun om det inte finns skäl att sekretessbelägga delar. Detta enligt reglerna i tryckfrihetsförordningen och offentlighets- och sekretesslagen.

15.7 Hur ska konsekvensbedömning följas upp?

Den personuppgiftsansvarige ska vid behov genomföra en översyn för att bedöma om behandlingen genomförs i enlighet med konsekvensbedömningen avseende dataskydd åtminstone när den risk som behandlingen medför förändras. Personuppgiftsansvarige bör regelbundet och kontinuerligt se över och omvärdera sina personuppgiftsbehandlingar för att bedöma om det bör genomföras en ytterligare konsekvensbedömning i fall om förhållanden har ändrats. Till exempel kan riskerna ha ändrats så att behandlingen nu sannolikt leder till en hög risk fast den inte gjorde det tidigare. Konsekvensbedömningen är en pågående process.

15.8 Sammanfattande beskrivning av stegen



16. Personuppgiftsincident

En personuppgiftsincident är 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. Personuppgiftsincident kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks. Exempel:

- Diskriminering, identitetsstöld, bedrägeri, skadlig ryktesspridning.
- Finansiell förlust.
- Brott mot sekretess eller tystnadsplikt.

En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personuppgifter har:

- Blivit förstörda, oavsiktligt eller olagligt.
- Gått förlorade på annat sätt eller ändrats.
- Kommit i orätta händer/röjts till någon obehörig.

Exempel på personuppgiftsincidenter:

- a) Obehörig part har fått tillgång till personuppgifterna, till exempel om någon har skickat personuppgifter till mottagare som inte skulle ha uppgifterna.
- b) Datorer som innehåller personuppgifter har förlorats eller stulits.
- c) Någon har ändrat personuppgifter utan tillstånd.
- d) Personuppgifterna är inte tillgängliga för den som behöver dem, och det leder till negativa effekter för de registrerade personerna.

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

För att hantera en personuppgiftsincident ska det finnas en incidentgrupp bestående av IT-chefen, säkerhetsansvarig och jurist (eller motsvarande funktion), samt samordnare och dataskyddsombud.



17. Gallring

Personuppgifter får inte bevaras längre än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Det innebär att uppgifter kan behöva gallras fortlöpande eller att andra åtgärder kan krävas (t ex att åtkomstbegränsningar införs). Det kan dessutom finnas krav i annan författning på att bevara uppgifter viss tid, t ex för redovisnings- eller arkivändamål. Genom en gallringspolicy eller någon annan plan för dokumenthantering kan dessa åtgärder tydliggöras och införas i verksamheten.

Även personuppgifter i ostrukturerat material såsom i dokument på servrar, i en enkel lista, på webbplatser o s v behöver raderas när ändamålet med behandlingen är uppfyllt. För att hantera detta behöver en bedömning alltid göras för vilket ändamål exempelvis ett e-postmeddelande eller dokument ska sparas och var (t ex kundregistret, ärendet etc).

Det finns ingen bestämd tidsgräns för hur länge personuppgifter får behandlas, utan tidsgränsen måste bedömas från fall till fall, utifrån följande:

- Gällande regelverk för arkivering.
- Pågående relation med den registrerade som kan påverka gallringstiden.
- Ändamålet med behandlingen kan tala för en längre gallringstid.

Det är framförallt viktigt att gällande gallringsrutiner följs så att inte handlingar med personuppgifter blir kvar i hyllor eller arkiv på ett sätt som inte kan motiveras.



18. Checklista

Varje personuppgiftsansvarig bör uppfylla följande GDPR krav:

- Utse ett dataskyddsbud och anmäla det till tillsynsmyndigheten.
- Se till att alla medarbetare genomgått utbildning om dataskyddsförordningen.
- Se till alla medarbetare genomfört inventering av personuppgifter som de behandlar.
- Se till alla medarbetare gjort en utvärdering av de personuppgifter som de behandlar.
- Se till att identifiera laglig grund för behandling av personuppgifter.
- Se till att identifiera ändamål med varje behandling av personuppgifter.
- Se till att det finns ett register med behandlingar av personuppgifter.
- Se till att alla registrerade får information om hur deras personuppgifter behandlas.
- Se till att det finns en uppdaterad gallringspolicy samt att medarbetare använder den.
- Se till att ha alla rutiner på plats för att kunna respektera de registrerades rättigheter såsom att få kopia på den information som behandlas, korrigering eller radering etc.
- Se till att alla medarbetare är utbildade i vilka rutiner (processer) som gäller.
- Se till att våra processer uppfyller tillämpliga säkerhetskrav.
- Se till att alla medarbetare som upprättar personuppgiftsbiträdesavtal använder standard personuppgiftsbiträdesavtal som uppfyller GDPR krav.
- Se till att det finns personuppgiftsbiträdesavtal med alla personuppgiftsbiträden och att de är uppdaterade.
- Se till att det utses minst en samordnare för varje personuppgiftsansvarig.
- Se till att personuppgiftsincidenter hanteras enligt GDPR samt anmäls till tillsynsmyndigheten inom 72 timmar.

Vanliga brister vid tillämpning av GDPR:

De typiska bristerna när det gäller efterlevnaden av personuppgiftslagen (tidigare lagstiftning) och som återkommande påpekats i Datainspektionens tillsynsbeslut har varit följande:

- Otillräcklig information ges till de registrerade, eller information som inte är korrekt när det gäller exempelvis ändamålet för behandlingen.
- Personuppgiftsbiträdesavtal saknas.
- Registerförteckning saknas.
- Överföring till tredje land sker i strid med lag.
- Gallringsrutiner saknas och personuppgifter behandlas under för lång tid.
- Otillräcklig behörighetsbegränsning finns för åtkomst till data/dokument.
- Rutiner för att lämna information till de registrerade efter begäran saknas.
- Se över behandlingen av särskilda kategorier av uppgifter, behandling av personnummer och behandling av särskilda kategorier av personuppgifter ("känsliga personuppgifter").
- Se över om det genomförs konsekvensbedömningar samt vidta åtgärder.
- Se över om det sker överföring till tredje länder och vidta åtgärder.



Bilageförteckning

1. Länder som omfattas av GDPR
2. Register författningar och speciallagstiftning
3. Personuppgiftsbiträdesavtal



Bilaga 1 - Länder som omfattas av GDPR

Det är viktigt att komma ihåg att institutionens, organisationens eller näringslivets fysiska läge är inte lika viktigt för att fastställa behovet av att följa GDPR som den fysiska platsen där den registrerade befinner sig - den person vars uppgifter samlas in, bearbetas eller lagras.

Lagstiftningen gäller i EU medlemsstater och EES länder, men den kommer att få en global inverkan då organisationer i andra länder kommer att ha tillgång till och behandla personuppgifter som tillhör registrerade som är medborgare i EU och EES länder.

EU, Europeiska unionens 28 medlemsländer:

Bulgarien	Grekland	Malta	Spanien
Belgien	Irland	Nederländerna	Storbritannien
Cypern	Italien	Polen	Sverige
Danmark	Kroatien	Portugal	Tjeckien
Estland	Lettland	Rumänien	Tyskland
Finland	Litauen	Slovakien	Ungern
Frankrike	Luxemburg	Slovenien	Österrike

EES, Europeiska Ekonomiska Samarbetsområdets tre medlemsländer:

Island Liechtenstein Norge



Bilaga 2 - Registerförfattningar och speciallagstiftning

För behandling av känsliga personuppgifter krävs lagstöd. Sådant stöd och andra regler om hur personuppgifter ska behandlas på respektive område finns i registerförfattningar och speciallagstiftning. Ett urval av sådan lagstiftning presenteras här.

Registerförfattningar mm

Socialtjänst, vård och omsorg

- Lagen (2001:454) om behandling av personuppgifter inom socialtjänsten (SoLPuL).
- Förordning (2001:637) om behandling av personuppgifter inom socialtjänsten.
- Patientdatalagen (2008:355)
- Patientdataförordning (2008:360)

Observera att dataskyddsförordningen och tillhörande författningar inte är tillämpliga på hela socialtjänstens område. **Dataskyddsdirektivet och brottsdatalagen (2018:1177) är istället tillämpliga** vid arbete i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.¹ Av propositionerna 2017/18 s 183-184 och 2017/18:232 s 431 framgår att dataskyddsdirektivet och brottsdatalagen gäller när statens institutionsstyrelse verkställer slutna ungdomsvård och när socialnämnder verkställer straffrättsliga påföljder samt vård enligt lag (1998:870) om vård av missbrukare i vissa fall, LVM.

Utbildning

- Skollagen (2010:800).
- Förordning (2006:39) om register och dokumentation vid fullgörandet av kommunernas aktivitetsansvar för ungdomar

Val

- Lagen (2001:183) om behandling av personuppgifter i verksamhet med val och folkomröstningar samt förordning (2002:61) om behandling av personuppgifter i verksamhet med val (Länsstyrelsen registeransvarig)

Andra lagar som anpassats till dataskyddsförordningen

En rad lagar har anpassats till dataskyddsförordningen och relaterar direkt till den. Det gäller till exempel olika civilrättsliga lagar på bl.a. fastighetsrättens område har anpassats,

¹ Av 1 kap. 3 § SoLPuL framgår att den lagen (och GDPR, samt dataskyddslagen) *inte* tillämpas vid behandling av personuppgifter som avses i artikel 2.2 d GDPR, se också skäl 19, samma förordning.



registerförfattningar på arbetsmarknadsområdet har anpassats, lagar inom miljö- och energidepartementets område har anpassats. Detsamma gäller lagar inom skatt, tull och exekution samt på finansmarknadsområdet. Det har också kommit en ny kamerabevakningslag.



Bilaga 3 – Personuppgiftsbiträdesavtal

Denna förlaga till personuppgiftsbiträdesavtal är direkt hämtat från SKR:s webbplats/hemsida, Adress:

<https://skr.se/ekonomijuridikstatistik/juridik/offentlighetsekretessarkiv/dataskyddsförordningengdpr/informationsinsatserkringdataskyddsförordningen/personuppgiftsbitrade.16046.html>

På hemsidan finns också ytterligare information om avtalet.

Om personuppgiftsbiträdesavtalet på SKR:s hemsida uppdateras, ska den uppdaterade versionen från hemsidan användas.



Innehållsförteckning

1. PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER	3
2. DEFINITIONER	3
3. BAKGRUND OCH SYFTE.....	5
4. BEHANDLING AV PERSONUPPGIFTER OCH SPECIFIKATION	5
5. DEN PERSONUPPGIFTSANSVARIGES ANSVAR	5
6. PERSONUPPGIFTSBITRÄDETS ÅTAGANDEN.....	6
7. SÄKERHETSÅTGÄRDER.....	6
8. SEKRETESS/TYSTNADSPLIKT	7
9. GRANSKNING, TILLSYN OCH REVISION	8
10. HANTERING AV RÄTTELSER OCH RADERING M.M.	8
11. PERSONUPPGIFTSINCIDENTER	9
12. UNDERBITRÄDE.....	9
13. LOKALISERING OCH ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND.....	10
14. ANSVAR FÖR SKADA I SAMBAND MED BEHANDLING.....	10
15. LAGVAL OCH TVISTLÖSNING	11
16. PUB-AVTALETS TECKNANDE, AVTALSTID OCH UPPSÄGNING	11
17. ÄNDRINGAR OCH UPPSÄGNING MED OMEDELBAR VERKAN M.M.	11
18. ÅTGÄRDER VID PUB-AVTALETS UPPHÖRANDE	12
19. MEDDELANDE INOM RAMEN FÖR DETTA PUB-AVTAL OCH INSTRUKTIONER.....	12
20. KONTAKTPERSONER	12
21. ANSVAR FÖR UPPGIFTER OM PARTERNA OCH KONTAKTPERSONER SAMT KONTAKTUPPGIFTER	13
22. PARTERNAS UNDERTECKNANDEN AV PUB-AVTALET.....	13



PERSONUPPGIFTSBITRÄDESAVTAL

Avtal enligt Allmänna dataskyddsförordningen EU 2016/679, art. 28.3¹

1. PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER

Personuppgiftsansvarig	Personuppgiftsbiträde
<i>[Organisationens fullständiga namn]</i>	<i>[Organisationens fullständiga namn]</i>
Organisationsnummer	Organisationsnummer
<i>[Organisationens organisationsnummer]</i>	<i>[Organisationens organisationsnummer]</i>
Postadress	Postadress
<i>[Organisationens postadress]</i>	<i>[Organisationens postadress]</i>
Kontaktperson för administration av detta personuppgiftsbiträdesavtal	Kontaktperson för administration av detta personuppgiftsbiträdesavtal
Namn: <i>[Kontaktpersonens Förnamn och Efternamn]</i> E-post: <i>[Kontaktpersonens e-postadress]</i> Tfn: <i>[Kontaktpersonens telefonnummer]</i>	Namn: <i>[Kontaktpersonens Förnamn och Efternamn]</i> E-post: <i>[Kontaktpersonens e-postadress]</i> Tfn: <i>[Kontaktpersonens telefonnummer]</i>
Kontaktperson för parternas samarbete om dataskydd	Kontaktpersoner för parternas samarbete om dataskydd
Namn: <i>[Kontaktpersonens Förnamn och Efternamn]</i> E-post: <i>[Kontaktpersonens e-postadress]</i> Tfn: <i>[Kontaktpersonens telefonnummer]</i>	Namn: <i>[Kontaktpersonens Förnamn och Efternamn]</i> E-post: <i>[Kontaktpersonens e-postadress]</i> Tfn: <i>[Kontaktpersonens telefonnummer]</i>

2. DEFINITIONER

Utöver de begrepp som definieras i löptext, i detta personuppgiftsbiträdesavtal, ska dessa definitioner oavsett om de används i plural eller singular, i bestämd eller obestämd form, ha nedanstående innebörd när de anges med versal som begynnelsebokstav.

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,
------------	---

¹ Allmänna dataskyddsförordningen EU 2016/679 föreskriver att det ska finnas ett skriftligt avtal om Personuppgiftsbiträdets Behandling av Personuppgifter för Den personuppgiftsansvariges räkning.



	lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.
Dataskyddslagstiftning	Avser all integritets- och personuppgiftslagstiftning, samt all annan eventuell lagstiftning (inklusive förordningar och föreskrifter), som är tillämplig på den personuppgiftsbehandling som sker enligt detta PUB-avtal, inklusive nationell sådan lagstiftning och EU-lagstiftning.
Personuppgiftsansvarig	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamål och medlen för Behandlingen av Personuppgifter.
Instruktion	De skriftliga instruktioner som närmare anger föremål, varaktighet, art och ändamål, typ av Personuppgifter samt kategorier av Registrerade och särskilda behov som omfattas av Behandlingen.
Logg	Logg är resultatet av Loggning.
Loggning	Loggning är ett kontinuerligt insamlande av uppgifter om den Behandling av Personuppgifter som utförs enligt detta PUB-avtal och som kan knytas till en enskild fysisk person.
Personuppgiftsbiträde	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som Behandlar Personuppgifter för den Personuppgiftsansvariges räkning.
Personuppgift	Varje upplysning som avser en identifierad eller identifierbar fysisk person, 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 lokaliseringssuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.
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.
Registrerad	Fysisk person vars Personuppgifter Behandlas.
Tredje land	En stat som inte ingår i Europeiska unionen (EU) eller inte är ansluten till Europeiska ekonomiska samarbetsområdet (EES).



Underbiträde	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som i egenskap av underleverantör till Personuppgiftsbiträdet Behandlar Personuppgifter för Personuppgiftsansvariges räkning.
--------------	--

3. BAKGRUND OCH SYFTE

3.1 Med detta Personuppgiftsbiträdesavtal ("PUB-avtalet") reglerar den Personuppgiftsansvarige Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige. PUB-avtalets syfte är att säkerställa den Registrerades fri- och rättigheter vid Behandlingen, i enlighet med vad stadgas i Allmänna dataskyddsförordningen EU 2016/679 ("Dataskyddsförordningen"), art. 28.3.

3.2 PUB-avtalet utgör ett självständigt avtal om Behandlingen. När PUB-avtalet utgör ett av flera avtalsdokument inom ramen för ett annat avtal benämns det andra avtalet "Huvudavtalet" i PUB-avtalet.

3.3 För det fall något av det som stadgas i kap. 1, 16, 17, 18.2, 19 – 22 i PUB-avtalet regleras på annat sätt i Huvudavtalet ska Huvudavtalets reglering ha företräde.

3.4 PUB-avtalets information, i form av bestämmelser och andra uppgifter som påverkar PUB-avtalets tillämpning, samt PUB-avtalets hänvisningar till sådan information, t.ex. lagstiftning (inklusive förordningar och föreskrifter), avser vid var tid gällande sådan information.

4. BEHANDLING AV PERSONUPPGIFTER OCH SPECIFIKATION

4.1 Den Personuppgiftsansvarige utser härmed Personuppgiftsbiträdet att utföra Behandlingen för den Personuppgiftsansvariges räkning enligt vad som stadgas i detta PUB-avtal.

4.2 Den Personuppgiftsansvarige ska ge Instruktioner till Personuppgiftsbiträdet om hur det ska utföra Behandlingen.

4.3. Personuppgiftsbiträdet får endast utföra Behandlingen i enlighet med PUB-avtalet och vid var tid gällande Instruktioner.

5. DEN PERSONUPPGIFTSANSVARIGES ANSVAR

5.1 Den Personuppgiftsansvarige ansvarar för att det vid var tid finns laglig grund för Behandlingen och för att utforma korrekta Instruktioner så att Personuppgiftsbiträdet och Underbiträdet kan fullgöra sitt eller sina uppdrag enligt detta PUB-avtal och Huvudavtal i förekommande fall.



5.2 Den Personuppgiftsansvarige ska utan onödigt dröjsmål informera Personuppgiftsbiträdet om förändringar i Behandlingen vilka påverkar Personuppgiftsbitrådets skyldigheter enligt Dataskyddslagstiftningen.

5.3 Den Personuppgiftsansvarige ansvarar för att informera Registrerade om Behandlingen och för att tillvarata Registrerades rättigheter enligt Dataskyddslagstiftningen samt vidta varje annan åtgärd som åligger den Personuppgiftsansvarige enligt Dataskyddslagstiftningen.

6. PERSONUPPGIFTSBITRÄDETS ÅTAGANDEN

6.1 Personuppgiftsbiträdet förbinder sig att endast utföra Behandlingen i enlighet med PUB-avtalet och Instruktioner samt att följa Dataskyddslagstiftningen. Personuppgiftsbiträdet förbinder sig även att fortlöpande hålla sig informerad om gällande rätt på området.

6.2 Personuppgiftsbiträdet ska vidta åtgärder för att skydda Personuppgifterna mot alla slag av Behandlingar som inte är förenliga med PUB-avtalet, Instruktioner och Dataskyddslagstiftningen.

6.3 Personuppgiftsbiträdet åtar sig säkerställa att samtliga fysiska personer som arbetar under dess ledning följer PUB-avtalet och Instruktioner samt att de fysiska personerna informeras om relevant lagstiftning.

6.4 Personuppgiftsbiträdet ska på begäran från den Personuppgiftsansvarige bistå denne med att säkerställa att skyldigheterna enligt Dataskyddsförordningen, art. 32-36, fullgörs och svara på begäran om utövande av den Registrerades rättigheter i enlighet med Dataskyddsförordningen, kap. III, med beaktande av typen av Behandling och den information som Personuppgiftsbiträdet har att tillgå.

6.5 För det fall att Personuppgiftsbiträdet finner att Instruktioner är otydliga, i strid med Dataskyddslagstiftningen eller saknas och Personuppgiftsbiträdet bedömer att nya eller kompletterande Instruktioner är nödvändiga för att genomföra sina åtaganden ska Personuppgiftsbiträdet utan dröjsmål informera den Personuppgiftsansvarige, tillfälligt upphöra med Behandlingen och invänta nya Instruktioner.

6.6 För det fall att den Personuppgiftsansvarige förser Personuppgiftsbiträdet med nya eller ändrade Instruktioner ska Personuppgiftsbiträdet, utan onödigt dröjsmål från mottagandet, meddela den Personuppgiftsansvarige huruvida genomförandet av de nya Instruktionerna föranleder förändrade kostnader för Personuppgiftsbiträdet.

7. SÄKERHETSÅTGÄRDER

7.1 Personuppgiftsbiträdet ska vidta alla tekniska och organisatoriska säkerhetsåtgärder som krävs för att förhindra Personuppgiftsincidenter, genom att säkerställa att Behandlingen uppfyller kraven i Dataskyddsförordningen och att den Registrerades rättigheter skyddas.



7.2 Personuppgiftsbiträdet ska fortlöpande säkerställa att den tekniska och organisatoriska säkerheten i samband med Behandlingen medför en lämplig nivå av konfidentialitet, integritet, tillgänglighet och motståndskraft.

7.3 Eventuella tillkommande eller ändrade krav på skyddsåtgärder från den Personuppgiftsansvarige, efter parternas tecknande av PUB-avtalet, ska betraktas som nya Instruktioner enligt PUB-avtalet.

7.4 Personuppgiftsbiträdet ska genom behörighetskontrollsystem endast ge åtkomst till Personuppgifterna för sådana fysiska personer som arbetar under Personuppgiftsbitrådets ledning och som behöver åtkomsten för att kunna utföra sina arbetsuppgifter.

7.5 Personuppgiftsbiträdet åtar sig att kontinuerligt Logga åtkomst till Personuppgifterna enligt PUB-avtalet i den utsträckning det krävs enligt Instruktionen. Loggar får gallras först fem (5) år efter Loggningstillfället om inte annat anges i Instruktionen. Loggar ska omfattas av erforderliga skyddsåtgärder, i enlighet med Dataskyddslagstiftningen.

7.6 Personuppgiftsbiträdet ska systematiskt testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa Behandlingens säkerhet.

8. SEKRETESS/TYSTNADSPLIKT

8.1 Personuppgiftsbiträdet och samtliga fysiska personer som arbetar under dess ledning ska vid Behandlingen iaktta såväl sekretess som tystnadsplikt. Personuppgifterna får inte nyttjas eller spridas för andra ändamål, vare sig direkt eller indirekt, såvida inte annat avtalats.

8.2. Personuppgiftsbiträdet ska tillse att samtliga fysiska personer som arbetar under dess ledning, vilka deltar i Behandlingen, är bundna av sekretessförbindelse avseende Behandlingen. Detta krävs dock inte om dessa redan omfattas av en straffsanktionerad tystnadsplikt som följer av lag. Personuppgiftsbiträdet åtar sig även att tillse att det finns sekretessavtal med Underbiträdet samt sekretessförbindelser mellan Underbiträdet och samtliga fysiska personer som arbetar under dess ledning, vilka deltar i Behandlingen.

8.3 Personuppgiftsbiträdet ska skyndsamt underrätta den Personuppgiftsansvarige om eventuella kontakter med tillsynsmyndighet avseende Behandlingen. Personuppgiftsbiträdet har inte rätt att företräda den Personuppgiftsansvarige eller agera för den Personuppgiftsansvariges räkning gentemot tillsynsmyndigheter i frågor avseende Behandlingen.

8.4 Om den Registrerade, tillsynsmyndighet eller tredje man begär information från Personuppgiftsbiträdet vilken rör Behandlingen, ska Personuppgiftsbiträdet informera den Personuppgiftsansvarige om saken. Information om Behandlingen får inte lämnas till den Registrerade, tillsynsmyndighet eller tredje man utan skriftligt medgivande från den Personuppgiftsansvarige, såvida det inte framgår av tvingande lag att information ska lämnas.



Personuppgiftsbiträdet ska bistå med förmedling av den informationen som omfattas av ett medgivande eller lagkrav.

9. GRANSKNING, TILLSYN OCH REVISION

9.1 Personuppgiftsbiträdet ska utan onödigt dröjsmål, på den Personuppgiftsansvariges begäran, tillhandahålla den information om tekniska och organisatoriska säkerhetsåtgärder som den Personuppgiftsansvarige behöver för att kunna fastställa att Personuppgiftsbiträdet uppfyller sina åtaganden enligt PUB-avtalet och Dataskyddsförordningen, art. 28.3 h.

9.2 Personuppgiftsbiträdet åtar sig att minst en (1) gång om året granska säkerheten avseende Behandlingen genom en egenkontroll för att säkerställa att Behandlingen följer PUB-avtalet. Resultatet av sådan egenkontroll ska på begäran delges den Personuppgiftsansvarige.

9.3 Den Personuppgiftsansvarige äger rätt att, själv eller genom annan av denne utsedd tredje part (som inte får vara en konkurrent till Personuppgiftsbiträdet), följa upp att Personuppgiftsbiträdet uppfyller PUB-avtalets, Instruktionernas och Dataskyddslagstiftningens krav. Personuppgiftsbiträdet ska vid sådan granskning bistå den Personuppgiftsansvarige, eller den som utför granskningen i den Personuppgiftsansvariges ställe, med dokumentation, tillgång till lokaler, IT-system och andra tillgångar som behövs för att kunna granska Personuppgiftsbitrådets efterlevnad av PUB-avtalet, Instruktioner och Dataskyddslagstiftningen. Den Personuppgiftsansvarige ska säkerställa att personal som genomför granskningen är underkastade sekretess eller tystnadsplikt enligt lag eller avtal.

9.4 Personuppgiftsbiträdet äger alternativt till vad som stadgas i punkterna 9.2-9.3, rätt att erbjuda andra tillvägagångssätt för granskning av Behandlingen, exempelvis granskning genomförd av oberoende tredje part. Den Personuppgiftsansvarige ska i sådant fall äga rätt, men inte skyldighet, att tillämpa detta alternativa tillvägagångssätt för granskning. Vid sådan granskning ska Personuppgiftsbiträdet ge den Personuppgiftsansvarige eller en tredje part den assistans som behövs för utförandet av granskningen.

9.5 Personuppgiftsbiträdet ska bereda tillsynsmyndighet, eller annan myndighet som har laglig rätt till det, möjlighet att göra tillsyn enligt myndighetens begäran i enlighet med vid var tid gällande lagstiftning, även om sådan tillsyn annars skulle stå i strid med bestämmelserna i PUB-avtalet.

9.6 Personuppgiftsbiträdet ska tillförsäkra den Personuppgiftsansvarige rättigheter gentemot Underbiträdet vilka motsvarar den Personuppgiftsansvariges samtliga rättigheter gentemot Personuppgiftsbiträdet enligt kap. 9 i PUB-avtalet.

10. HANTERING AV RÄTTELSE OCH RADERING M.M.

10.1 För det fall den Personuppgiftsansvarige begärt rättelse eller radering på grund av Personuppgiftsbitrådets felaktiga Behandling ska Personuppgiftsbiträdet vidta lämplig åtgärd utan onödigt dröjsmål, senast inom trettio (30) dagar, från det att Personuppgiftsbiträdet



mottagit erforderlig information från den Personuppgiftsansvarige. När den Personuppgiftsansvarige begärt radering får Personuppgiftsbiträdet endast utföra Behandling av den aktuella personuppgiften som ett led i processen för radering.

10.2 Om tekniska och organisatoriska åtgärder (t.ex. uppgraderingar eller felsökningar) vidtas av Personuppgiftsbiträdet i Behandlingen, vilka kan väntas påverka Behandlingen, ska Personuppgiftsbiträdet informera den Personuppgiftsansvarige skriftligt om detta i enlighet med vad stadgas om meddelanden i 19 kap. i PUB-avtalet. Informationen ska lämnas i god tid innan åtgärderna vidtas.

11. PERSONUPPGIFTSINCIDENTER

11.1 Personuppgiftsbiträdet ska ha förmåga att återställa tillgängligheten och tillgången till Personuppgifterna i rimlig tid vid en fysisk eller teknisk incident enligt Dataskyddsförordningen, art. 32.1 c.

11.2 Personuppgiftsbiträdet åtar sig att med beaktande av Behandlingens art, och den information som Personuppgiftsbiträdet har att tillgå, bistå den Personuppgiftsansvarige med att fullgöra dennes skyldigheter vid en Personuppgiftsincident beträffande Behandlingen. Personuppgiftsbiträdet ska på den Personuppgiftsansvariges begäran även bistå med att utreda misstankar om eventuell obehörig Behandling och/eller åtkomst till Personuppgifterna.

11.3 Vid Personuppgiftsincidenter, vilka Personuppgiftsbiträdet fått vetskap om, ska Personuppgiftsbiträdet utan onödigt dröjsmål skriftligen underrätta den Personuppgiftsansvarige om händelsen. Personuppgiftsbiträdet ska med beaktande av typen av Behandling och den information som Personuppgiftsbiträdet har att tillgå tillhandahålla den Personuppgiftsansvarige en skriftlig beskrivning av Personuppgiftsincidenten.

Beskrivningen ska redogöra för:

1. Personuppgiftsincidentens art och, om möjligt, de kategorier och antalet Registrerade som berörs samt kategorier och antalet personuppgiftsposter som berörs,
2. de sannolika konsekvenserna av Personuppgiftsincidenten, och
3. åtgärder som har vidtagits eller föreslagits samt åtgärder för att mildra Personuppgiftsincidentens potentiella negativa effekter.

11.4 Om det inte är möjligt för Personuppgiftsbiträdet att tillhandahålla hela beskrivningen samtidigt, enligt punkt 11.3 i PUB-avtalet, får beskrivningen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

12. UNDERBITRÄDE

12.1 Personuppgiftsbiträdet ansvarar fullt ut för Underbitrådets Behandling gentemot den Personuppgiftsansvarige.



12.2 Personuppgiftsbiträdet äger rätt att anlita ett nytt underbiträde. När Personuppgiftsbiträdet avser att anlita ett nytt underbiträde ska Personuppgiftsbiträdet säkerställa underbitrådets kapacitet och förmåga att uppfylla sina skyldigheter enligt Dataskyddslagstiftningen. Personuppgiftsbiträdet ska skriftligen meddela den Personuppgiftsansvarige om

1. underbitrådets namn, organisationsnummer och säte (adress och land),
2. vilken typ av uppgifter och kategorier av Registrerade som behandlas, och
3. var Personuppgifterna ska behandlas.

12.3 Personuppgiftsbiträdet äger rätt att upphöra med att anlita Underbiträdet. När Personuppgiftsbiträdet upphör med att anlita Underbiträdet ska Personuppgiftsbiträdet skriftligen meddela den Personuppgiftsansvarige om att det upphör med att anlita Underbiträdet.

12.4 Personuppgiftsbiträdet åtar sig att teckna ett skriftligt personuppgiftsbiträdesavtal med det nya underbiträdet och säkerställa att det nya underbiträdet åläggs samma skyldigheter som Personuppgiftsbiträdet åläggs enligt detta PUB-avtal.

12.5 Personuppgiftsbiträdet ska på den Personuppgiftsansvariges begäran översända en kopia av det personuppgiftsbiträdesavtal som Personuppgiftsbiträdet tecknat med Underbiträdet.

12.6 Den Personuppgiftsansvarige äger inom 30 dagar rätt att invända mot Personuppgiftsbitrådets anlitanande av ett nytt underbiträde och att, med anledning av sådan invändning, säga upp detta PUB-avtal att upphöra i enlighet med vad stadgas i PUB-avtalet, punkt 17.4.

13. LOKALISERING OCH ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND

13.1 Personuppgiftsbiträdet ska säkerställa att Personuppgifterna hanteras och lagras inom EU/EES av en fysisk eller juridisk person som är etablerad inom EU/EES, om inte PUB-avtalets parter kommer överens om något annat.

13.2 Personuppgiftsbiträdet äger endast rätt att överföra Personuppgifter till Tredje land för Behandling (t.ex. service, support, underhåll, utveckling, drift eller liknande hantering) om den Personuppgiftsansvarige på förhand skriftligen godkänt sådan överföring och utfärdat Instruktioner för detta ändamål.

13.3 Överföring till Tredje land för Behandling enligt PUB-avtalet, punkt 13.2, får endast ske om den är förenlig med Dataskyddslagstiftningen och uppfyller de krav på Behandlingen vilka ställs i PUB-avtalet och Instruktioner.

14. ANSVAR FÖR SKADA I SAMBAND MED BEHANDLING

14.1 Vid ersättning för skada i samband med Behandling som, genom fastställd dom eller förlikning, ska utgå till den Registrerade på grund av överträdelse av bestämmelse i PUB-



avtalet, Instruktioner och/eller tillämplig bestämmelse i Dataskyddslagstiftningen ska art. 82 i Dataskyddsförordningen tillämpas.

14.2 Sanktionsavgifter enligt Dataskyddsförordningen, art. 83, eller Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning 6 kap. 2 § ska bäras av den av PUB-avtalets parter som påförts en sådan avgift.

14.3 Om endera part får kännedom om omständighet som kan leda till skada för motparten ska parten omedelbart informera motparten om förhållandet och aktivt arbeta tillsammans med motparten för att förhindra och minimera sådan skada.

14.4 Oaktat vad sägs i Huvudavtalet gäller detta PUB-avtal, punkter 14.1 och 14.2, före andra regler om fördelning mellan Parterna av krav sinsemellan såvitt avser Behandlingen.

15. LAGVAL OCH TVISTLÖSNING

För detta avtal gäller svensk rätt. Eventuell tolkning eller tvist i anledning av PUB-avtalet, som parterna inte kan lösa på egen hand, ska avgöras av svensk allmän domstol.

16. PUB-AVTALETS TECKNANDE, AVTALSTID OCH UPPSÄGNING

16.1 PUB-avtalet gäller från och med den tidpunkt PUB-avtalet undertecknats av båda parter och tills vidare. Parterna äger ömsesidig rätt att säga upp PUB-avtalet att upphöra med trettio (30) dagars varsel.

17. ÄNDRINGAR OCH UPPSÄGNING MED OMEDELBAR VERKAN M.M.

17.1 Endera part i PUB-avtalet äger rätt att påkalla omförhandling av PUB-avtalet om motpartens ägarförhållanden ändras väsentligt eller om tillämplig lagstiftning, eller tolkningen av den, ändras på ett för Behandlingen avgörande sätt. Påkallande av omförhandling enligt första meningen innebär inte att PUB-avtalet till någon del upphör att gälla utan endast att en omförhandling om PUB-avtalet ska påbörjas.

17.2 Tillägg till, och ändringar i, PUB-avtalet ska vara skriftliga och undertecknade av båda parter.

17.3 När någon av parterna får kännedom om att motparten agerar i strid med PUB-avtalet, Instruktioner och/eller Dataskyddslagstiftningen, ska parten utan dröjsmål meddela motparten om agerandet. Därefter äger parten rätt att med omedelbar verkan upphöra att utföra sina förpliktelser enligt PUB-avtalet till den tidpunkt motparten förklarat att agerandet upphört och förklaringen accepterats av den part som påtalat agerandet.

17.4 Om den Personuppgiftsansvarige invänder mot Personuppgiftsbitrådets anlitan av ett nytt underbiträde, enligt detta PUB-avtal, punkt 12.6, har den Personuppgiftsansvarige rätt att



säga upp PUB-avtalet att upphöra med omedelbar verkan. Om Personuppgiftsbiträdet Behandlar Personuppgifterna efter den tidpunkt som anges i punkt 18.2 gäller vad stadgas i punkter 18.3-18.4.

18. ÅTGÄRDER VID PUB-AVTALETS UPPHÖRANDE

18.1 Vid uppsägning av PUB-avtalet ska den Personuppgiftsansvarige utan onödigt dröjsmål begära att Personuppgiftsbiträdet överlämnar samtliga Personuppgifter till den Personuppgiftsansvarige eller raderar dem, enligt dennes önskemål. Om Personuppgifterna överlämnas ska det ske i ett öppet och standardiserat format. Med samtliga Personuppgifter avses alla Personuppgifter vilka har omfattats av Behandlingen samt annan tillhörande information såsom Loggar, Instruktioner, systemlösningar, beskrivningar och andra handlingar som Personuppgiftsbiträdet erhållit genom informationsutbyte enligt PUB-avtalet.

18.2 Överlämning och radering enligt PUB-avtalet, punkt 18.1, ska vara utförda senast trettio (30) dagar räknat från den tidpunkt uppsägning gjorts enligt detta PUB-avtal, punkt 16.1

18.3 Behandling som utförs av Personuppgiftsbiträdet efter den tidpunkt som stadgas i punkt 18.2 är att betrakta som en otillåten Behandling.

18.4 Bestämmelser om sekretess/tystnadsplikt i 8 kap. PUB-avtalet ska fortsätta gälla även om PUB-avtalet i övrigt upphör av gälla.

19. MEDDELANDEN INOM RAMEN FÖR DETTA PUB-AVTAL OCH INSTRUKTIONER

19.1 Meddelanden om PUB-avtalet och dess administration inklusive uppsägning ska skickas till respektive parts kontaktperson för PUB-avtalet.

19.2 Meddelanden om parternas samarbete om dataskydd, gällande Behandlingen, ska skickas till respektive parts kontaktperson för parternas samarbete om dataskydd.

19.3 Meddelanden inom ramen för PUB-avtalet och Instruktioner ska skickas skriftligt. Ett meddelande ska anses ha kommit fram till mottagaren senast en (1) arbetsdag efter att meddelandet har skickats.

20. KONTAKTPERSONER

20.1 Parterna ska utse var sin kontaktperson för PUB-avtalet.

20.2 Parterna ska utse var sin kontaktperson för parternas samarbete om dataskydd.



21. ANSVAR FÖR UPPGIFTER OM PARTERNA OCH KONTAKTPERSONER SAMT KONTAKTUPPGIFTER

21.1 Varje part ansvarar för att de uppgifter som anges i 1 kap. i PUB-avtalet alltid är aktuella. Ändring av uppgifter i 1 kap. ska meddelas skriftligt enligt punkt 19.1 i PUB-avtalet.

22. PARTERNAS UNDERTECKNANDEN AV PUB-AVTALET

22.1 Detta PUB-avtal tillhandahålls antingen i digitalt format för elektroniskt tecknande eller i pappersformat för tecknande med penna. Om PUB-avtalet tillhandahålls i digitalt format utgår punkter 22.2-22.3.

22.2 Den Personuppgiftsansvariges undertecknande av PUB-avtalet

Ort

Datum

.....

.....

Undertecknande

.....

.....

Namnförtydligande

22.3 Personuppgiftsbiträdets undertecknande av PUB-avtalet

Ort

Datum

.....

.....

Undertecknande

.....

.....

Namnförtydligande



Versionshantering

Version	Datum	Förändringar	Ansvarig
1.1	2018-12-19	10.1, 14.1, 18.2,	PR



Upprättad: 2020-08-25
Diarienummer: SN.2020.32

Socialnämnden

Rapportering av ej verkställda gynnande biståndsbeslut enligt SoL och LSS

Förslag till beslut i kommunstyrelsen

1. Rapporteringen godkänns.

Sammanfattning

Socialnämnden är skyldig att rapportera till IVO om beviljat bistånd enligt SoL och insatser enligt LSS som inte har verkställts tre månader efter beslut.

Ärendebeskrivning

För andra kvartalet 2020 finns det 3 insatser enligt LSS som inte har verkställt tre månader efter beslut.

Det första beslutet rör en brukare som beviljades personlig assistans 2020-01-22, beslutet har dock verkställts 2020-06-01 genom extern utförare.

Det andra beslutet rör en brukare som beviljades bostad med särskild service 2020-01-29, beslutet verkställdes dock 2020-08-24 genom extern placering.

Det tredje beslutet rör en brukare som beviljades kontaktperson 2020-03-04, beslutet är ännu ej verkställt pga. resursbrist; har ej lyckats hitta lämplig utförare.

Vidare finns det 1 beviljat bistånd enligt SoL som inte är verkställt under rapporteringsperioden. Beslutet rör en brukare som beviljades särskilt boende 2020-03-09, biståndet verkställdes dock 2020-08-24.

Beslutsunderlag

1. Tjänsteskrivelse 2020-08-25

Veronica Östlin
Förvaltningschef

Ida Claesson
Utredare

Sändlista

- ~ Kommunstyrelsen
- ~ Kommunfullmäktige

Upprättad: 2020-09-23
Diarienummer: SN.2020.1

Socialnämnden

Redovisning av delegationsbeslut

Sammanfattning

Socialnämnden har överlåtit sin beslutanderätt till tjänsteman enligt av socialnämnden antagen delegationsordning. Dessa beslut skall redovisas till socialnämnden.

Redovisningen innebär inte att socialnämnden får ompröva eller fastställa delegeringsbesluten. Däremot står det socialnämnden fritt att återkalla lämnad delegering.

Delegationsbesluten i sin helhet finns tillgängliga hos kommunledningskontoret. Tiden för överklagande av beslut som fattats med stöd av delegationen börjar löpa fr.o.m att socialnämndens protokoll justeras och anslagsbevis är uppsatt på kommunens digitala anslagstavla. Detta gäller dock inte myndighetsärenden där tiden börjar löpa från det datum då sökanden fått del av besluten.

Från och med maj 2013 innehåller inte redovisningen av delegationsbeslut uppgifter om vem som initierat respektive delegationsbeslut. Eftersom uppgift om initierare (namn och adress) kan omfattas av sekretess i vissa ärenden och då personer med skyddad identitet inte ska röjas, har dessa uppgifter tagits bort.

- ~ Förteckning över delegationsbeslut 2020-08-19 – 2020-09-22
- ~ Förteckning över anställningar 2020-08-01 – 2020-08-31



Beslutsperiod:

Ärende: SN.2020.13
Styrning
Vidaredelegering

Beslutsdatum: 2020-08-28

Beslut: Beslut om vidaredelegering Tf förvaltningschef, §1: Fastställt

Socialnämnden

Förteckning över avtal om månadsavlönade tillsvidareanställningar utfärdade mellan 2020-08-01 – 2019-08-31

Undersköterska
Organisation: Hemtjänst Björnlunda
Tillsvidare, From: 2020-10-01
Deltid (75,00%)
Utfärdat av: Monica Petersson, Enhetschef Ekhagen

Kvalitetsutvecklare
Organisation: Stab Administration och bistån
Tillsvidare, From: 2020-09-01
Heltid
Utfärdat av: Veronica Östlin, Förvaltningschef

Undersköterska
Organisation: Särskilt boende Ekhagen
Tillsvidare, From: 2020-10-01
Deltid (75,00%)
Utfärdat av: Monica Petersson, Enhetschef Ekhagen

Undersköterska
Organisation: Hemtjänst Björnlunda
Tillsvidare, From: 2020-10-01
Deltid (75,00%)
Utfärdat av: Monica Petersson, Enhetschef Ekhagen

Förteckning över avtal om månadsavlönade visstidsanställningar utfärdade mellan 2020-08-01 – 2020-08-31

Vårdbiträde
Organisation: Särskilt boende Strandhagen
Allm visstidsanställning, 2020-09-01 - 2020-09-30
Deltid (75,00%)
Utfärdat av: Anders Hallinder, Chef

Undersköterska
Organisation: Särskilt boende Strandhagen
Allm visstidsanställning, 2020-09-01 - 2020-09-30
Deltid (95,00%)
Utfärdat av: Anders Hallinder, Chef

Vårdbiträde
Organisation: Särskilt boende Strandhagen
Allm visstidsanställning, 2020-09-01 - 2020-09-30
Deltid (50,00%))
Utfärdat av: Anders Hallinder, Chef

Handläggare
Organisation: Personlig assistans
Allm visstidsanställning, 2020-08-24 - 2020-12-31
Heltid
Utfärdat av: Anders Hallinder, Chef

Undersköterska
Organisation: Särskilt boende Strandhagen
Allm visstidsanställning, 2020-09-01 - 2020-09-30
Heltid
Utfärdat av: Anders Hallinder, Chef

Undersköterska
Organisation: Särskilt boende Strandhagen
Allm visstidsanställning, 2020-09-01 - 2020-09-30

Deltid (75,00%)

Utfärdat av: Anders Hallinder, Chef

Arbetshandledare

Organisation: Daglig verksamhet Samba

Vikariat, 2020-08-24 - 2020-12-31

Deltid (75,00%)

Utfärdat av: Camilla Andersson, Enhetschef

Upprättad: 2020-09-23
Diarienummer: SN.2020.2

Socialnämnden

Anmälningssärenden

Sammanfattning

Information och meddelanden som inkommer till kommunen och som socialförvaltningen bedömer vara av vikt att redovisa för socialnämnden, utgör anmälningssärenden. Anmälningssärendena i sin helhet finns tillgängliga hos kanslienheten samt hos sekreteraren under sammanträdet.

- ~ Protokoll från sociala utskottet, 2020-08-19
- ~ Protokoll från nämnden för samverkan kring socialtjänst och vård, 2020-09-11
- ~ Protokollsutdrag från Nämnden för samverkan kring socialtjänst och vård, Återrapport – Nattfasta/Dygnsmätning
- ~ Handlingsplan för fallprevention i Sörmland

