ESLÖVS KOMMUN

RIKTLINJER FÖR BEHANDLING AV PERSONUPPGIFTER

Dokumentet är antaget av kommunstyrelsen 2021-11- 30 att gälla från och med den 2022-01-01. Det riktar sig till hela kommunen. Ses över för revidering senast december 2025. Kontaktperson: Kommunledningskontoret, juridiska avdelningen. Dnr KS.2020.0414

Innehåll

1 Inledning
Dessa riktlinjer beskriver de övergripande ramar som anställda och förtroendevalda ska tänka på vid behandling av personuppgifter. De grundar sig på den nya allmänna dataskyddsförordningen (EU) 2016/679, som i vardagligt tal kallas för GDPR.

Utgångspunkten är att anställda och förtroendevalda ska kunna hantera de personuppgifter som behövs i deras arbete/uppdrag, samt inse vikten av att försöka tänka riskmedvetet och bli bättre på att uppmärksamma de risker som kan uppstå i samband med behandling av personuppgifter. Detta för att förstå vikten av lämpliga skyddsåtgärder och på så sätt minska risken för att personuppgifter hamnar i orätta händer, förstörs eller inte går att nå när det finns ett behov av det.

Det är bra att vara medveten om att det finns en konflikt mellan yttrandefrihet och GDPR. I Sverige regleras detta bland annat i den svenska dataskyddslagen.

GDPR och den svenska dataskyddslagen gäller inte om det strider mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen[1].

2 Begreppsförklaringar
2.1 Dataskyddslagstiftning
Dataskyddslagstiftning kallas de lagar som reglerar behandling av personuppgifter.

2.2 Behandling
Med behandling avses i stort sett allt som görs med personuppgifterna. Det kan exempelvis röra sig om insamling, registrering, lagring och spridning av personuppgifter. Lagring kan till exempel ske lokalt på en dator, i en pärm, på en samarbetsyta eller på en server. Andra exempel på behandlingar är läsning, användning, utlämning genom överföring, radering och förstöring.

2.3 Personuppgifter
En personuppgift är information som kan identifiera en (fysisk) person som är i livet. Uppgiften kan enskilt eller i kombination med andra uppgifter knytas till en person som gör att det går att förstå vem personen är.

[1] 1 kap 7§ första stycket dataskyddslagen.

Exempel på direkta personuppgifter är namn, personnummer och fotografier.

Exempel på indirekta personuppgifter är fastighetsbeteckning, GPS-position, kontonummer och användarnamn.

Krypterade uppgifter och olika slags elektroniska identiteter, som exempelvis IP-nummer och cookies, räknas också som personuppgifter om de kan kopplas till fysiska personer. Även information som har kodats, krypterats eller pseudonymiserats kan vara en personuppgift om det med hjälp av anslutande uppgifter går att förstå vem det rör sig om.

Bilder, filmer och ljudupptagningar av individer kan vara personuppgifter även om inga namn nämns.

Vissa kategorier av personuppgifter är offentliga uppgifter, enligt offentlighetsprincipen. Detta trots att de kategoriseras som känsliga eller integritetskänsliga/extra skyddsvärda personuppgifter. Det innebär att det måste finnas tillräckliga säkerhetsåtgärder på plats när dessa uppgifter ska lämnas ut.

I rubrikerna nedan beskrivs skillnaden mellan integritetskänsliga/extra skyddsvärda personuppgifter och känsliga personuppgifter.

2.3.1 Skyddsvärda/integritetskänsliga personuppgifter

Personnummer/Samordningsnummer
Personnummer (ÅÅMMDD-XXXX) och samordningsnummer är extra skyddsvärda personuppgifter. Samordningsnummer är ett tillfälligt identitetsnummer för personer som inte är folkbokförda i landet men som har kontakt med landets myndigheter. Användningen av samordnings- och personnummer regleras i den svenska dataskyddslagen[2]. Där står det bland annat att personnummer endast får användas om det är nödvändigt att säkerställa att det är rätt person som behandlas, om behandlingen kan vara motiverad utifrån ändamålet eller om det finns ett inhämtat samtycke.

Slentrianmässig användning och onödig exponering av person- och samordningsnummer ska undvikas. Om personnummer används i en behandling ska det motiveras. Om det inte kan motiveras så bör det inte

[2] Dataskyddslagen 3 kap. 10§.

användas. Där det går kan exempelvis födelsedatum (ÅÅMMDD) användas istället.

Personnummer ska som huvudregel inte heller användas som användaridentitet vid inloggning i olika typer av verksamhetssystem. Om det finns behov av att använda personnummer som inloggning så ska dataskyddsombudet tillfrågas.

Barns uppgifter
Barns personuppgifter är extra skyddsvärda, eftersom barn kan ha svårare att förutse riskerna med att lämna ifrån sig sina uppgifter samt förstå sina rättigheter.

Andra integritetskänsliga uppgifter
Förutom personnummer/samordningsnummer och barns personuppgifter så finns det många andra integritetskänsliga personuppgifter som är extra skyddsvärda, så som:

- löneuppgifter
- uppgifter om lagöverträdelser
- värderande uppgifter, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler
- information som rör någons privata sfär
- uppgifter om sociala eller ekonomiska förhållanden
- personuppgifter som omfattas av sekretess eller tystnadsplikt

2.3.2 Känsliga personuppgifter

I GDPR finns det särskilda kategorier av personuppgifter. I vardagligt tal kallas de för känsliga personuppgifter. Det är uppgifter om:

- etnicitet (exempelvis modersmål, födelseland eller tolkbehov)
- politiska åsikter (exempelvis medlemskap i politiskt parti)
- religiös eller filosofisk övertygelse (exempelvis medlem i religiöst samfund, särskilda kostönskemål)
- medlemskap i fackförening
- genetiska eller biometriska uppgifter som identifierar en individ
- (exempelvis dna-analys, ansiktsigenkänning, fingeravtryck)
- hälsa (exempelvis sjukfrånvaro, behov av hjälpmedel, behov bostadsanpassning, handikapparkeringstillstånd)
- sexualliv eller sexuell läggning

Foton betraktas inte som känsliga uppgifter såvida de inte är föremål för ny teknik som exempelvis att de behandlas med hjälp av ansiktsigenkänningsteknik.

Känsliga personuppgifter kräver i regel ett starkare skydd än andra vanliga personuppgifter, och får endast behandlas vid vissa undantag. Läs mer om detta under avsnitt *5.2 Känsliga personuppgifter*.

3 Roller

3.1 Den registrerade

Den registrerade är den person vars personuppgifter behandlas inom våra olika verksamheter. Exempel på registrerade är exempelvis anställda, förtroendevalda, förskolebarn, elever, brukare, äldre och medborgare i kommunen.

3.2 Personuppgiftsansvarig

Kommunfullmäktige, kommunstyrelsen och nämnderna är ansvariga för sina respektive verksamhetsområden. De har det yttersta juridiska ansvaret för att all behandling av personuppgifter som sker under deras respektive verksamhetsansvar efterlever GDPR/dataskyddslagstiftningen.

Kommunstyrelsen är även personuppgiftsansvarig för de personuppgiftsbehandlingar som är gemensamma för hela kommunen.

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 olika skyldigheter.

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

Personuppgiftsansvaret är omfattande och följande lista tjänar som vägledning för vad som ingår. Listan är inte uttömmande.

Personuppgiftsansvarig ansvarar bland annat för att:

- all behandling av personuppgifter följer rådande dataskyddslagstiftning,

- försäkra sig om att förvaltningen och verksamheten har en ändamålsenlig organisation med tillräckliga resurser och dokumenterad ansvarsfördelning,
- säkerställa att medarbetarna har nödvändig kompetens för att kunna följa dataskyddslagstiftningen,
- all behandling av personuppgifter dokumenteras i en registerförteckning,
- inträffade incidenter hanteras enligt GDPR,
- det finns uppdaterade personuppgiftsbiträdesavtal med alla personuppgiftsbiträden,
- risk och konsekvensbedömningar utförs över behandlingar som innebär hög risk för den enskildes fri- och rättigheter,
- det finns lämpliga tekniska och organisatoriska säkerhetsåtgärder för varje behandling av personuppgifter,
- det finns ett utsett dataskyddsombud, som anmälts till tillsynsmyndigheten samt att ombudet har förutsättningar och tillräcklig kunskap som krävs för utförande av uppdraget.

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

3.2.1 Förvaltningarnas roll

Förvaltningarna utför det praktiska dataskyddsarbetet och hjälper den personuppgiftsansvarige med att uppfylla sitt ansvar.

Det är viktigt att det finns kompetens och personella resurser för att GDPR ska kunna efterlevas. Dataskyddsarbete är ett ständigt systematiskt pågående arbete hos samtliga anställda i alla verksamheter där personuppgifter behandlas.

3.3 Personuppgiftsbiträde

Ett personuppgiftsbiträde behandlar personuppgifter på uppdrag av den personuppgiftsansvarige. Exempel på en biträdessituation är när en IT-leverantör behandlar personuppgifter genom att tillhandahålla support till ett system eller en tjänst.

3.3.1 Personuppgiftsbiträdesavtal

För att ett personuppgiftsbiträde ska få behandla personuppgifter måste ett personuppgiftsbiträdesavtal upprättas i enlighet med artikel 28 i GDPR. Biträdesavtalet är en del av tjänsteavtalet, och ska vara med redan i

upphandlingsprocessen. I upphandlingar ska kommunens egen standardmall för personuppgiftsbiträdesavtal bifogas förfrågningsunderlaget.

Avtalet reglerar hur hantering av personuppgifter ska ske. Biträdet får inte använda personuppgifterna för egna syften, exempelvis för statistik eller för förbättring av den egna produkten. Avtalet ska säkerställa att personuppgiftsbiträdet upprätthåller lämplig teknisk och organisatorisk säkerhet i enlighet med gällande dataskyddsrätt.

Om personuppgiftsbiträdet anlitar ett underbiträde är det den personuppgiftsansvariges skyldighet att säkerställa att det anlitade underbiträdet följer personuppgiftsbiträdesavtalet.

Personuppgiftsbiträdesavtal mellan olika nämnder i Eslövs kommun hanteras av den rättsakt som ligger som bilaga i policyn för systematiskt dataskyddsarbete. Detta innebär att i de fall där det finns en biträdesrelation mellan olika nämnder så behöver det inte skrivas något avtal dem emellan. Notera dock att det kan finnas scenarion där ett gemensamt personuppgiftsansvar mellan två eller fler av kommunens nämnder kan förekomma. I detta fall ska ansvarsfördelningen för behandlingarna dokumenteras så att det tydligt går att se vem som är personuppgiftsansvarig för vilken behandling.

3.4 Dataskyddsombud

Dataskyddsombudets ställning och arbetsuppgifter styrs av lagstiftning. Dataskyddsombudet agerar självständigt och får inte ta emot instruktioner eller bli föremål för sanktioner för att ha utfört sina arbetsuppgifter.

Dataskyddsombudet informerar och ger råd till den personuppgiftsansvarige om skyldigheterna enligt GDPR. Dataskyddsombudet övervakar även efterlevnad av GDPR samt ger råd vid konsekvensbedömningar. Den personuppgiftsansvarige ska säkerställa att dataskyddsombudet involveras i alla frågor som rör skyddet av personuppgifter.

Varje personuppgiftsansvarig har en skyldighet att utse ett dataskyddsombud och anmäla det till tillsynsmyndigheten.

3.5 Dataskyddssamordnare

Kommunstyrelsen och nämnderna i Eslövs kommun ska enligt policyn för systematiskt dataskyddsarbete[3] utse en eller flera lokala dataskyddssamordnare som löpande ska samordna arbetet kring GDPR på sin respektive förvaltning. Namnet på utsedd dataskyddssamordnare ska meddelas till dataskyddsombudet, men ska inte anmälas till tillsynsmyndigheten.

Rollen går att kombinera med andra arbetsuppgifter om det bedöms rimligt. Dataskyddssamordnaren är en stödfunktion. Ansvaret för att lagstiftningen efterlevs vilar alltid på den personuppgiftsansvarige och ansvaret kan inte delegeras.

Dataskyddssamordnaren stöttar verksamhet, ledning och den personuppgiftsansvarige genom att lämpligtvis men inte uteslutande:

- samordna dataskyddsfrågor och vara dataskyddsombudets kontaktperson,
- informera och ge råd i frågor som rör dataskydd, som exempelvis registerförteckning, personuppgiftsbiträdesavtal, säkerhetsåtgärder med mera,
- delta i Eslövs kommuns nätverk för dataskydd
- kommunicera kommunövergripande, och förvaltningsspecifika
- styrdokument inom dataskyddsområdet,
- övervaka efterlevnaden av lagstiftningen, och informera sin förvaltningsledning om de rättsliga kraven inte efterlevs eller riskerar att inte efterlevas, samt rapportera detta till dataskyddsombudet,
- prioritera och leda arbetet kring personuppgiftsincidenter,
- stödja förvaltningens arbete med risk- och konsekvensbedömningar.

3.6 Övriga chefer och medarbetare

Samtliga medarbetare har ett ansvar för att behandlingen av personuppgifter utförs i enlighet med dessa riktlinjer. Varje chef har ett ansvar att förmedla vikten av att följa gällande styrdokument.

4 Behandling av personuppgifter

I kommunens policy för systematiskt dataskyddsarbete listas GDPR:s grundläggande principer enligt artikel 5. För att behandling av personuppgifter ska vara laglig måste principerna efterlevas. Detta gäller vid

[3] KS.2019.0494.

all personuppgiftsbehandling, både vid en ny eller vid en större förändring i en befintlig behandling.

5 Laglig grund

Utgångspunkten vid all behandling av personuppgifter är alltid att börja med att fråga sig varför personuppgifterna behövs? Är det till exempel för att säkerställa att det är rätt person som erbjuds barnomsorg, skola eller får ekonomiskt bistånd? Om det är nödvändigt att använda personuppgifterna för att kunna utföra sitt myndighetsuppdrag är också den lagliga grunden enligt GDPR uppfylld. Det viktiga är att det finns en laglig grund enligt GDPR innan personuppgifterna samlas in. GDPR har sex lagliga grunder och för verksamheterna i Eslövs kommun innebär det oftast att någon av följande tre grunder ska användas:

- behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som den personuppgiftsansvarige har
- behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning
- behandlingen är nödvändig för att fullgöra ett avtal eller vidta åtgärder på begäran av den registrerade inför ett avtal

Övriga lagliga grunder i GDPR är:

- behandlingen är nödvändig för att skydda ett grundläggande intresse för den registrerade eller annan fysisk person
- berättigat intresse – ovanligt att denna används av myndigheter men det finns exempel på detta
- samtycke - ska användas med försiktighet av offentliga myndigheter. Detta då det i de flesta fallen blir en ojämn maktbalans mellan den registrerade och den personuppgiftsansvarige och samtycket kan då bedömas som ogiltigt

5.1 Särskilt om samtycke

Ett samtycke innebär att den registrerade godtar behandling av personuppgifter som rör honom eller henne. En förutsättning för ett giltigt samtycke är att den som är personuppgiftsansvarig kan visa att den registrerade har fått tydlig information och har gjort ett fritt, aktivt val att samtycka. Det finns alltså speciella villkor som ska vara uppfyllda för att ett samtycke ska anses som giltigt enligt GDPR.

Det finns ingen tydlig reglering av samtycke för minderåriga. Enligt den svenska dataskyddslagen kan unga över 13 år i vissa situationer själva

lämna sitt samtycke. Generellt verkar detta dock gälla vid informationssamhällets tjänster som till exempel, sociala medier, appar och spel. Något som borde vara ovanligt inom kommunens verksamhet. Detta innebär att samtycke generellt inte kan inhämtas från unga, utan istället krävs vårdnadshavarens samtycke.

5.2 Känsliga personuppgifter

Känsliga personuppgifter får enligt undantagen i artikel 9.2 a-j i GDPR och 3 kap 2-7§§ dataskyddslagen enbart behandlas om något av följande uppfylls:

- vid uttryckligt samtycke
- om uppgifterna offentliggjorts av den registrerade
- för att den personuppgiftsansvariga ska kunna fullgöra sina skyldigheter inom arbetsrätten och inom områdena social trygghet och socialt skydd
- den registrerades vitala intressen ska kunna skyddas
- ideella organisationers behandling av medlemmars personuppgifter (politiskt, filosofiskt, religiöst, fackligt syfte)
- för att fastställa eller tillvarata rättsliga anspråk eller domstols rättskipande verksamhet
- viktigt allmänt intresse
- hälso- och sjukvård och social omsorg
- allmänt intresse på folkhälsoområdet
- när det är nödvändigt av skäl som hör samman med förebyggande
- hälso- och sjukvård och yrkesmedicin
- vid bedömning av en arbetstagares arbetskapacitet
- när rättsliga anspråk ska kunna fastställas, göras gällande eller
- försvaras
- för medicinska diagnoser

6 Registerförteckning

En del av personuppgiftsansvaret innebär att den personuppgiftsansvarige behöver säkerställa att deras respektive verksamheter för register över alla de personuppgiftsbehandlingar som utförs inom det egna ansvarsområdet.

Registret är ett levande dokument som vid behov ska revideras.
I artikel 30 i GDPR står det vilka uppgifter som registerförteckningen ska innehålla.

För att kunna uppfylla GDPR:s grundläggande princip om ansvarsskyldighet och för att kunna ha en viss spårbarhet rekommenderar dataskyddsombudet även att registerförteckningen innehåller:

- vilken laglig grund behandlingen har
- var personuppgifterna finns lagrade, exempelvis på filserver, i system, på papper etc.
- uppgifter om personuppgiftsbiträde anlitats, samt om PUB-avtal finns
- namn eller beskrivning på behandlingen

7 Den registrerades rättigheter

Rättigheterna är avsedda för att de registrerade ska få information om när och hur deras personuppgifter behandlas och för att de ska få en ökad kontroll och självbestämmande över sina egna uppgifter.

Vid en begäran från en registrerad ska myndigheten svara senast inom en (1) månad efter mottagen begäran. För de fall där den registrerades begäran inte kan tillmötesgås helt eller delvis, ska ett avslagsbeslut[4] fattas och överklagandehänvisning ska bifogas beslutet[5] .

I avsnitt 7.1–7.7 listas de olika rättigheterna som den registrerade har. Utövandet av rättigheterna baserar sig på vilken laglig grund enligt GDPR som personuppgifterna behandlas på, därför inleds varje rättighet med vilken laglig grund som är giltig för just den rättigheten.

7.1 Rätt till information

Den registrerade har rätt till information oavsett vilken laglig grund som personuppgifterna behandlas på. Informationsskyldigheten gäller vid följande tillfällen.

a) **När personuppgifter samlas in direkt från den registrerade.** Information enligt artikel 13 i GDPR ska lämnas vid insamlingstillfället.
b) **Uppgifterna har tagits emot av en annan mottagare.** Information enligt artikel 14 i GDPR ska lämnas till den registrerade inom en rimlig period, men senast inom en månad.
c) **Om redan insamlade personuppgifter kommer att användas för ett annat syfte (ändamål) än för vilket de samlades in.**

[4] Vilka beslut som kan överklagas framgår av 7 kap. 2 § dataskyddslagen (2018:2018).
[5] Förvaltningslagen 33 §.

Ny information som förklarar ändamålet med den nya behandlingen måste lämnas till den registrerade innan behandlingen påbörjas. Detta för att den registrerade ska kunna invända mot behandlingen.

d) **De registrerade behöver också informeras aktivt om det görs väsentliga ändringar i behandlingen.**
e) **Vid vissa incidenter, beroende på incidentens allvarlighetsgrad och sammanhang.**

Information enligt anvisningar i artikel 34.2 ska lämnas utan dröjsmål.

På intranätet finns det mallar som kan användas för att uppfylla informationsplikten enligt artikel 13 och 14. Varje nämnd ansvarar för att informationen är korrekt i förhållande till de enskilda behandlingarna inom dess verksamhetsområde.

7.1.1 Undantag från informationsskyldigheten

Om information samlas in direkt från den registrerade så behöver informationen inte lämnas om den:

- den registrerade redan förfogar över informationen

I de fall där informationen samlas in från någon annan än den registrerade så behöver information inte lämnas i nedanstående fall:

- om det innebär en omöjlig eller oproportionerlig ansträngning som avsevärt försvårar uppfyllandet av målen (om detta skäl används behöver det beskrivas varför verksamheten inte bedömer att det är nödvändigt att lämna informationen)
- utelämnandet eller mottagandet av uppgifterna är föreskrivet i lag
- det finns lagstadgad sekretess (information kan inte ske om det finns uppgifter som inte får lov att röjas)

7.2 Rätt till tillgång – registerutdrag

Rätten till tillgång kallas också rätten till registerutdrag och den gäller oavsett vilken laglig grund som personuppgifterna behandlas på.

En enskild person har rätt att vända sig till kommunen för att få ut en sammanställning över vilka personuppgifter som myndigheten behandlar om personen samt på vilket sätt uppgifterna behandlas. Syftet är att personen ska få en ökad insyn i den behandling som sker, för att hen ska kunna kontrollera behandlingens laglighet.

Utdraget ska bland annat innehålla vilka uppgifter som behandlas om den registrerade, hur uppgifterna behandlas, var uppgifterna kommer ifrån, ändamålet med behandlingen och till vilka mottagare eller kategorier av mottagare uppgifterna lämnats ut. Registerutdraget ska tillhandahållas kostnadsfritt och vara formulerat med ett enkelt och tydligt språk. Utdraget ska i normalfallet lämnas ut senast en månad från dess att begäran mottagits. Särskilda skäl måste föreligga om registerutdraget försenas.

Utlämnande av registerutdrag till den registrerade sker antingen genom post till folkbokföringsadress alternativt genom avhämtning i reception. Om registerutdraget innehåller känsliga personuppgifter och ska skickas genom post ska uppgifterna alltid skickas genom rekommenderat brev. Registerutdrag får aldrig skickas via e-post till den registrerade.

Observera! Det kan finnas omständigheter som medför att information i registerutdrag inte ska lämnas ut, till exempel på grund av bestämmelser i offentlighets- och sekretesslagen eller att ett utlämnande av informationen medför nackdelar för andra. Det är alltså viktigt att tänka på sekretessen!

7.3 Rätt till rättelse och radering

Personer har rätt att vända sig till kommunen med begäran om att få felaktiga personuppgifter rättade. Den enskilde har också rätt att begära att få komplettera med personuppgifter som saknas och som är relevanta, med hänsyn taget till ändamålet med behandlingen. Det finns också rätt för enskilda att begära att personuppgifter raderas.

I Sverige finns det en grundlagsskyddad rättighet, som styrs av tryckfrihetsförordningen, att ta del av allmänna handlingar. Den innebär att handlingar som upprättas eller inkommer till en myndighet ska registreras och lämnas ut till den som begär att få ta del av handlingen på det viset som handlingen inkommit eller upprättats om inte offentlighets- och sekretesslagen säger något annat. Arkivlagen reglerar att dessa allmänna handlingar ska bevaras om inte myndigheten beslutar på något annat sätt, det vill säga beslutar att en handling ska raderas genom ett gallringsbeslut.

Gallring innebär att handlingar/uppgifter tillhörande ett arkiv förstörs eller avlägsnas enligt på förhand fastställda kriterier. Gallringsbeslut är oftast fastställda i myndighetens informationshanteringsplan. Ovanstående bakgrund är viktig att tänka på när någon begär rättelse, komplettering eller radering av personuppgifter.

Möjligheterna att ändra i allmänna handlingar är mycket begränsade. Uppenbara skrivfel i myndighetsbeslut får rättas enligt 36§ Förvaltningslagen (2017:900), denna regel gäller inte skrivfel i nämndernas protokoll.

Det är alltså inte självklart att rättelse, komplettering eller radering är tillåtet hos en myndighet. Frågan måste först prövas utifrån det faktum att alla uppgifter som inkommer eller upprättats hos myndigheten är allmänna handlingar, om förvaltningslagens regler är tillämpliga samt om det finns gallringsbeslut. Vid gallring måste det enligt arkivlagen skrivas ett gallringsprotokoll.

Personuppgifter som registrerats baserat på ett samtycke kan återkallas med samtidig begäran om att personuppgifterna ska raderas. En sådan begäran innebär att behandlingen måste upphöra men personuppgifterna kan enbart raderas om det finns ett gallringsbeslut och uppgifterna inte har arkiverats. Därför är det viktigt att respektive nämnds informationshanteringsplan är uppdaterad på ett sådant sätt att information som inhämtas med den lagliga grunden samtycke ska gallras när samtycket återkallas.

Andra exempel på när begäran om radering kan ske är:

- om uppgifterna inte längre behövs för det ändamål som de samlades in för
- om personuppgiften har behandlats olagligt
- om radering krävs för att uppfylla en rättslig skyldighet.

Radering av ovannämnda exempel är tillåtet enbart om det är tillåtet enligt nämndens informationshanteringsplan att gallra uppgifterna.
Om uppgifter kompletteras, rättas eller raderas på den enskildes begäran måste det också informeras till de andra parter som kommunen fört över de felaktiga uppgifterna till. Detta gäller inte om det visar sig omöjligt eller skulle innebära en allt för betungande insats.

Om personuppgifterna dessutom har publicerats eller på annat sätt gjorts offentliga (exempelvis i ett socialt nätverk 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.

7.4 Rätt till begränsning av behandling

Rätt till begäran om begränsning gäller oavsett vilken laglig grund som uppgifterna behandlas på. Med begränsning avses att uppgifterna markeras och endast får användas för vissa avgränsade syften om det inte strider mot annan lagstiftning. Att utreda frågor om begränsning av behandling kommer sannolikt inte att vara vanligt förekommande och komplicerade att utreda av samma skäl som diskuterats i föregående avsnitt. Om det inkommer frågor gällande begränsning av behandling av personuppgifter så bör det ske ett samråd med dataskyddsombudet.

Rätt till begäran om begränsning gäller bland annat när den registrerade anser att uppgifterna är felaktiga. I sådana fall kan i vissa avseenden den registrerades personuppgifter begränsas/frysas under den tid det tar för verksamheten att utreda om uppgifterna är riktiga eller inte. När begränsningen upphör ska personen som begärt begränsningen informeras.

7.5 Rätt till dataportabilitet

Denna rättighet gäller enbart då personen själv har lämnat uppgifterna och när behandlingen grundar sig på den lagliga grunden samtycke eller avtal. Rätt till dataportabilitet innebär att den registrerade har rätt att få en kopia av personuppgifterna i strukturerat, allmänt använt och maskinläsbart format.

7.6 Rätt att göra invändningar

Den registrerade har rätt att invända mot personuppgiftsbehandling när personuppgifter behandlas på den lagliga grunden att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning.

Om en person invänder mot behandling får den personuppgiftsansvarige bara fortsätta med behandlingen om det finns skäl som väger tyngre än den registrerades intressen, rättigheter och friheter eller om behandlingen sker för fastställande, utövande eller försvar av rättsliga anspråk enligt dataskyddsförordningen.

Att utreda frågor där den registrerade invänder mot behandlingen kommer sannolikt inte att vara vanligt förekommande. De är dock komplicerade att utreda av samma skäl som diskuterats i avsnittet om rätt till rättelse och radering. Om det inkommer frågor gällande invändning av behandling av personuppgifter så bör det ske ett samråd med dataskyddsombudet.

7.7 Automatiserat individuellt beslutsfattande inbegripet profilering

Enligt GDPR har den registrerade rätt att inte bli föremål för ett beslut som enbart grundas på någon form av automatiserat beslutsfattande, inbegripet profilering[6], om beslutet kan ha rättsliga följder för den enskilde eller på liknande sätt i betydande grad påverkar honom eller henne.

Automatiserat beslutsfattande är förmågan att fatta beslut på teknisk väg, utan mänsklig inblandning, och kan vara tillåtet om det är nödvändigt för ett ingående eller fullgörande av avtal mellan den registrerade och den personuppgiftsansvarige, eller om den enskilde har gett sitt uttryckliga samtycke. Det kan även vara tillåtet enligt särskild lagstiftning, som exempelvis förvaltningslagen.

Informationsskyldigheten som beskrivs under avsnitt 7.2 gäller även för personuppgifter som behandlas på detta sätt.

Automatiserade beslut kan fattas med eller utan profilering. Omvänt kan profilering användas utan att det leder till ett automatiserat beslut.

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

Vid en behandling av personuppgifter som omfattar automatiserat beslutsfattande och/eller profilering bör dataskyddsombudet involveras i ett tidigt skede.

7.8 Rätt att lämna klagomål

Den registrerade har rätt att lämna klagomål som avser behandling av personuppgifter till personuppgiftsansvarig, dataskyddsombudet eller tillsynsmyndigheten.

8 Personuppgiftsincident

I GDPR definieras ”personuppgiftsincident” på följande sätt i artikel 4.12: ”*en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst*

[6] ”varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar” (artikel 4.4 i GDPR).

till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.”

Om personuppgifter blir ”förstörda” så innebär det att uppgifterna inte längre finns, alternativt existerar de i ett format som gör att de inte längre kan användas. En incident kan också uppstå om personuppgifter har ändrats, blivit korrupta eller inte längre är fullständiga.

En ”förlust” av personuppgifter bör tolkas som att uppgifterna fortfarande finns kvar, men att den personuppgiftsansvarige har förlorat kontrollen över eller åtkomsten till dem, eller inte längre innehar uppgifterna.

Obehörig behandling är om personuppgifter lämnas ut (eller åtkomst ges) till mottagare som inte är behöriga att motta (eller få åtkomst till) uppgifterna.

Om en incident inträffar så kan det innebära olika konsekvenser för de registrerade, så som risk för diskriminering, identitetstöld, bedrägeri, skadlig ryktesspridning, finansiell förlust eller brott mot sekretess och tystnadsplikt, men det behöver inte innebära det.

Om en incident innebär en sannolik risk för den registrerades rättigheter så ska den anmälas till tillsynsmyndigheten inom 72 timmar efter upptäckt, om det inte är osannolikt att incidenten medför en risk för personers fri- och rättigheter. Nämndens dataskyddsombud ska alltid informeras.

Se separata framtagna riktlinjer om hur personuppgiftsincidenter ska hanteras[7].

9 Konsekvensbedömning

Alla personuppgiftsbehandlingar bör analyseras i en risk- och konsekvensbedömning, där personuppgifterna ska klassificeras utifrån såväl dataskyddslagstiftning och offentlighets- och sekretesslagen som utifrån informationssäkerhet. Klassningen och analysen ligger till grund för vilka säkerhetskrav som ska ställas på administrativa och tekniska lösningar samt på fysisk säkerhet.

Om en personuppgiftsbehandling sannolikt leder till en hög risk för en persons rättigheter och friheter ska en konsekvensbedömning alltid utföras.

[7] KS.2018.0665.

En konsekvensbedömning kan behöva genomföras:

- innan en behandling av personuppgifter påbörjas
- om risken med en pågående behandling ändras
- för pågående behandlingar om det ännu inte har genomförts.

Konsekvensbedömningar ska alltså även utföras för behandlingar som påbörjats innan GDPR började gälla.
Kärnverksamheterna är de som måste ta det största ansvaret för arbetet med bedömningen. Detta eftersom de vet vilka personuppgifter de behandlar, hur dessa hanteras samt hur processerna i verksamheten ser ut. Förvaltningens dataskyddssamordnare ska involveras.

Dataskyddsombudet ska få möjlighet att lämna synpunkter på den utförda konsekvensbedömningen.

10 Nyanskaffning

Innan verksamheter börjar behandla personuppgifter i appar, system eller med hjälp av nya tekniska hjälpmedel är det viktigt att fastställa syftet med behandlingen av personuppgifter och den lagliga grunden enligt GDPR.

Personuppgifter som behandlas ska vara nödvändiga för syftet med behandlingen och beställaren ska säkerställa att personuppgifterna som samlas in är korrekta. Uppgifterna ska inte förvaras i en form som möjliggör identifiering under längre tid än nödvändigt. Lagring över längre perioder ska följa lagstadgade krav och riktlinjer. Vid bedömning av gallringsfrister i informationshanteringsplan ska principen om lagringsminimering beaktas. Att ta bort uppgifter ska följa regler och rutiner för rensning och gallring.

Säkerhet ska utgöras av *inbyggt dataskydd* och *dataskydd som standard*.

Inbyggt dataskydd innebär att hänsyn ska tas till dataskyddsreglerna redan vid utformning av IT-system och rutiner. Det är ett sätt att se till att kraven i GDPR uppfylls och att den registrerades rättigheter skyddas.

Dataskydd som standard innebär i korthet att den som behandlar personuppgifter ska se till att personuppgifter inte behandlas i onödan. Till exempel ska de förvalda inställningarna i en tjänst vara inställda så att inte mer information än nödvändigt samlas in, delas eller visas.

11 Säkerhetsåtgärder

Behandling av personuppgifter får endast ske om det finns lämpliga tekniska och organisatoriska säkerhetsåtgärder implementerade.

Tekniska åtgärder är exempelvis brandväggar, krypteringsfunktioner med mera, medan organisatoriska åtgärder exempelvis kan vara olika styrdokument som policys, riktlinjer och rutiner.

Känsliga personuppgifter kräver ofta den högsta säkerhetsnivån, men tänk på att även integritetskänsliga personuppgifter:

- kan kräva en högre säkerhetsnivå, och i vissa fall (exempelvis vid vissa sekretessbelagda personuppgifter) lika hög nivå som känsliga personuppgifter
- har betydelse för riskbedömningen när det görs konsekvensbedömning

Tillsynsmyndigheten har ställt krav på att starka säkerhetsåtgärder vidtas för sådana fall där integritetskänsliga uppgifter registreras så att de finns att nå över internet (öppna nät), exempelvis efter inloggning.

12 Överföring till tredje land

Överföring av personuppgifter till tredje land är när personuppgifter blir tillgängliga för någon i ett land utanför EU/EES-området. Det kan enligt tillsynsmyndigheten exempelvis vara:

- när ett dokument som innehåller personuppgifter skickas per e-post till någon i ett land utanför EU/EES
- när ett anlitat personuppgiftbiträde är beläget i ett land utanför EU/EES
- när någon utanför EU/EES ges 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

Obs! Däremot är det inte en tredjelandsöverföring att publicera något på internet förutsatt att webbplatsen lagras hos en internetleverantör som är etablerad inom EU/EES. För att överföra personuppgifter utanför EU/EES måste något av följande uppfyllas:

- det finns ett beslut från EU-kommissionen om att ett visst land utanför EU/EES säkerställer så kallad adekvat skyddsnivå

- lämpliga skyddsåtgärder har vidtagits av den som personuppgiftsansvarig genom till exempel bindande företagsbestämmelser (så kallade Binding Corporate Rules, BCR) eller standardavtalsklausuler (så kallade Standard Contractual Clauses, SCC). I vissa fall krävs det också att SCC kompletteras med utförd riskbedömning
- det kan också finnas andra särskilda situationer och enstaka fall, rådgör med nämndens dataskyddsombud i frågan

13 Personuppgifter i molntjänster

Innan personuppgifter lagras i en molntjänst är det viktigt att tänka på om lagringen i sig kommer att vara laglig och/eller lämplig.

Om personuppgiftsbiträdet eller något av dess underbiträden är bundna av regler i tredje land som inskränker på integritetsskyddet för en enskild, är det i de flesta fall både olämpligt och olagligt att använda sig av molntjänster för att behandla personuppgifter.

I de fall där personuppgifter ska behandlas i en molntjänst så är rekommendationen att alltid utföra en risk- och konsekvensbedömning.

14 Utbildning

Alla anställda ska genomgå en årlig utbildning inom dataskydd via e-learning. Närmaste chef är ansvarig för att följa upp att medarbetarna genomgår de utbildningar som tillhandahållas.

Utbildningar kan göras tillsammans på exempelvis APT:er eller enskilt. Det viktiga är att utbildningarna följs upp och registreras.

15 Bevara eller gallra

Det är inte GDPR eller den svenska dataskyddslagen som styr bevarande och gallring av personuppgifter i allmänna handlingar, utan det är i första hand regler i arkivlagen. Kommunstyrelsen och nämnderna är skyldiga att se till att allmänna handlingar arkiveras och bevaras. Enligt arkivpraxis räcker det att handlingarna sparas hos myndigheten för att de ska anses vara arkiverade. Ett arkiv kan alltså finnas tillgängligt i samma datasystem, men måste då enligt GDPR innehålla tekniska avgränsningar, såsom exempelvis begränsad åtkomst.

15.1 Lämpliga åtgärder för att skydda de registrerades rättigheter

Att kunna behandla personuppgifter vid hantering av allmänna handlingar har i svensk rätt sin grund i tryckfrihetsförordningen men också i offentlighets- och sekretesslagen, arkivlagen och förvaltningslagen. I Sverige finns det lagar och regler som är till för att skydda den enskildes integritet. Sekretess är ett exempel, informationssäkerhet, gallring och leverans till arkivmyndighet är en annan form av åtgärd.

Insamlade personuppgifter får lagras under längre tid för arkivändamål om det finns åtgärder som skyddar de registrerades rättigheter . Ett sätt att göra detta är exempelvis att begränsa åtkomsten till de uppgifter som kan anses inaktuella för verksamheten, genom ett avskiljande i systemet med begränsad åtkomst. Ett avskiljande räknas inte som gallring och kräver inget gallringsbeslut.

15.2 Gallring av personuppgifter

För att få avidentifiera (en form av gallring) eller för att förstöra (gallra) en allmän handling eller uppgifter i allmän handling krävs stöd i lag (inte GDPR) eller gallringsbeslut. Gallringsbeslut måste fattas av nämnd/myndighet. Enskild tjänsteman får aldrig besluta om gallring.
Vid gallring måste det också skrivas ett gallringsprotokoll.
Det finns två olika sätt att ta bort personuppgifter, antingen genom avidentifiering eller förstöring (gallring).

Avidentifiera (en form av gallring)

Att avidentifiera personuppgifterna innebär att avlägsna alla identifieringsmöjligheter så att de uppgifter som fortsättningsvis behandlas inte längre går att koppla samman med en fysisk person. Krypterade personuppgifter är inte avidentifierade så länge någon kan göra uppgifterna läsbara och därmed identifiera personen.

Förstöra (gallra)

Gallring innebär att handlingar/uppgifter som tillhör ett arkiv avlägsnas och förstörs enligt fastställda kriterier. Att förstöra personuppgifterna innebär att se till att de inte går att återskapa. Hur långtgående tekniska åtgärder som bör vidtas är bland annat beroende av informationens känslighet.

15.3 Informationshanteringsplan

Gallring inom kommunens verksamheter får inte ske utan att gallringen medges i, av den personuppgiftsansvarige, antagen informationshanteringsplan. Informationshanteringsplanen gäller både för digitala handlingar och fysiska handlingar. Av informations-

hanteringsplanen framgår även om speciallagstiftning anger särskild gallringsfrist (till exempel Patientdatalagen och SoL).
Varje arkivansvarig ansvarar för att informationshanteringsplanen revideras av arkivombudet vid behov och för att systematisk gallring av personuppgifter genomförs.

16 Utlämning av handlingar

GDPR hindrar inte kommunen att lämna ut en allmän handling enligt offentlighetsprincipen. Däremot behöver handlingen lämnas ut på ett säkert sätt. Om den som begär ut uppgifterna vill ha den digitalt måste en bedömning göras om uppgifterna kan lämnas ut på ett säkert sätt, annars får utlämningen ske på papper. Det finns inte någon skyldighet att lämna ut uppgifter enligt offentlighetsprincipen annat än på papper.

Vissa personuppgifter i ett dokument kan vara offentliga och andra sekretessbelagda. Det kan finnas behov av att maskera uppgifter innan handlingen lämnas ut. Maskering av sekretessbelagda uppgifter innebär dock ett nekande av att lämna ut de uppgifterna i handlingen. Det framgår av delegeringsordningen vem som har rätt att fatta beslut om att inte lämna ut de uppgifter eller den handling som är sekretessbelagd.

17 Personuppgifter i e-post

Att skicka e-post till eller från en personlig e-postlåda (förnamn.efternamn@eslov.se) är en behandling av personuppgifter, om e-postadressen kan kopplas till en fysisk person. Vid all behandling av personuppgifter i e-post är det viktigt att alltid tänka utifrån GDPR:s regel om uppgiftsminimering. Det vill säga, skriv inte in mer personuppgifter i e-postmeddelandet än vad som behövs.

E-posten är inte en lämplig permanent lagringsyta och e-post som innehåller personuppgifter som behöver fortsatt behandling bör överföras till ett dokument- och ärendehanteringssystem eller annan form av lagring, sedan ska e-postmeddelandet raderas enligt gällande rutiner. När e-post är mottagen beror det alltså på innehållet om och hur länge meddelandet får sparas. Externt inkommen e-post ska generellt anses som allmän handling och ska sparas en viss tid, alternativt gallras, se verksamhetens gällande informationshanteringsplan.

Vissa personuppgifter kan skickas till alla, exempel på sådana är epost-adress till jobbet, befattning, och för- och efternamn.

Integritetskänsliga personuppgifter bör inte skickas på e-post. I detta fall är det bättre att lägga dokumentet på en behörighetskontrollerad fildelningsyta eller i ett lämpligt system där endast de kollegor som behöver tillgång till dokument har behörighet.

Sekretessbelagda eller känsliga personuppgifter ska aldrig skickas via e-post om det inte finns tillräckliga skyddsåtgärder på plats som exempelvis krypterad e-post. Undantagna från denna regel är kontaktcenter som får skicka känsliga personuppgifter till interna e-postadresser, då de vidareförmedlar e-post som inkommit i kommunens brevlåda.

Vid besvarande av ett inkommande e-post som innehåller integritetskänsliga/känsliga personuppgifter är det viktigt att ta bort dessa uppgifter innan svaret skickas iväg.
Undvik att ansluta enheter till okända trådlösa eller fasta nätverk, använd istället mobilnätsuppkoppling för att hämta e-post.

18 Publicering på internet

18.1 Publicering av enskilda, anställdas och förtroendevaldas personuppgifter

Anställdas personuppgifter, såsom namn, titel, telefonnummer och e-postadress till arbetet och liknande arbetsplatsrelaterade personuppgifter får publiceras om det är nödvändigt för att informera om kommunens verksamhet. Den lagliga grunden för detta är att utföra en uppgift av allmänt intresse. Uppgifter om familjeförhållanden, bostadsadress, telefonnummer och fritidsintressen får inte publiceras.

Förtroendevaldas personuppgifter, såsom namn, typ av uppdrag, e-postadress (enbart @eslov.se) och telefonnummer som tillhandahålls av Eslövs kommun får publiceras, och den lagliga grunden för detta är att utföra en uppgift av allmänt intresse. Partitillhörighet får publiceras i de fall som den enskilde på ett tydligt sätt offentliggjort uppgifterna. Den förtroendevaldes privata telefonnummer eller mejladress får bara publiceras om samtycke finns. Om samtycket återkallas ska publiceringen upphöra. Uppgifter om familjeförhållanden, bostadsadress och fritidsintressen får inte publiceras.

Personuppgifter om enskilda, som till exempel namn, får publiceras om det finns stöd i någon av de lagliga grunderna för personuppgiftsbehandling och om dessa och övriga publicerade uppgifter, enskilt eller sammantaget, inte kan antas leda till att den registrerades personliga integritet kränks.

Följande får ej publiceras:

- Personnummer eller samordningsnummer.
- Uppgifter som omfattas av sekretess eller tystnadsplikt.
- Extra skyddsvärda personuppgifter, till exempel uppgifter om enskildas personliga förhållanden eller sådant som har en nära koppling till den enskildes privata sfär.
- Uppgifter om lagöverträdelser.
- Känsliga personuppgifter.

Uppgifter som exempelvis avslöjar politiska åsikter får dock publiceras om den enskilde själv på ett tydligt sätt offentliggjort uppgifterna och det i övrigt finns en laglig grund för behandlingen.

18.2 Publicering och spridning av foto och film

Foto/film på förtroendevalda samt anställda som har nyckelfunktioner får publiceras om syftet är att informera om kommunens verksamhet. Den lagliga grunden i detta fall är att utföra en uppgift av allmänt intresse.

Anställda som inte har nyckelfunktioner inom kommunen har ingen skyldighet att medverka på foton. Användning av samtycke som laglig grund kan komma anses ogiltigt med tanke på beroendeställning mellan arbetstagare och arbetsgivare. Lagstiftningen är dock oklar och om samtycke används bör det vara skriftligt dokumenterat och om ett återkallande sker så ska publiceringen upphöra.

Foto/film där enskilda medborgare, såväl vuxna som barn, inte kan identifieras (så kallade mingelbilder) får publiceras. Den lagliga grunden i detta fall är att utföra en uppgift av allmänt intresse. Om en medborgare kontaktar kommunen och anser att hen är identifierbar på en mingelbild och motsätter sig publiceringen bör publiceringen upphöra.

18.3 Kommunens digitala anslagstavla och webbdiarium

18.3.1 Kommunens anslagstavla

På kommunens digitala anslagstavla publiceras enbart uppgifter som styrs av lag, det kan till exempel vara protokoll och kallelser. Vid denna typ av publicering är det viktigt att iaktta uppgiftsminimering och

lagringsminimering för att uppfylla tillräckliga säkerhetsåtgärder enligt GDPR.

18.3.2 Kommunens webbdiarium

För webbdiarum gäller GDPR. Handlingar ska därför kontrolleras före publicering. En första kontroll ska göras i samband med registrering av handlingar i kommunens ärendehanteringssystem. Samma regler ska gälla för länkade dokument. Det är den som registrerar handlingen som ska kontrollera innehållet i handlingen. Handlingar kan även innehålla sekretessbelagda uppgifter. Dessa ska markeras i ärendehanteringssystemen vid registrering.

Innan publicering av handlingar sker ska ytterligare en kontroll göras, för att säkerställa att handlingarna inte innehåller personuppgifter som inte får publiceras. Personuppgifter som pekar ut en enskild får inte publiceras, undantaget är förtroendevalda i deras roll som förtroendevalda och tjänstemän i deras roll som tjänstemän. Detta innebär att handlingar kan publiceras men däremot kan enskilda personuppgifter behöva maskeras.

19 Sanktionsavgifter

Vid en överträdelse av GDPR och dataskyddslagen kan tillsynsmyndigheten utfärda en reprimand, föreläggande eller förbud mot den personuppgiftsansvarige. Tillsynsmyndigheten har även befogenhet att påföra administrativa sanktionsavgifter.

Vid överträdelse av följande bestämmelser (mindre allvarliga överträdelser) är maxbeloppet för en myndighet som högst 5 miljoner kronor.

Artikel	**Innehåll**
8,11, 25-39, 42 och 43 i GDPR	Personuppgiftsansvarigas/personuppgiftsbiträdens skyldigheter, exempelvis utförande av konsekvensbedömning
42-43 i GDPR	Certifieringsorganets skyldigheter
41.4 i GDPR	Övervakningsorganets skyldigheter

Vid överträdelser av följande bestämmelser (allvarliga överträdelser) är maxbeloppet för en myndighet som högst 10 miljoner kronor.

Artikel	Innehåll
5,6,7 och 9 i GDPR	Grundläggande principer, inklusive villkoren om samtycke
12-22 i GDPR	Registrerades rättigheter
44-49 i GDPR	Överföring av personuppgifter till tredjeland m.m.
3 kap. 10§ dataskyddslagen	Behandling av personnummer/samordningsnummer
58.2 c-h och j i GDPR	Underlåtenhet att rätta sig efter ett föreläggande från tillsynsmyndigheten.
58.1 i GDPR	Underlåtelse att ge tillsynsmyndigheten tillgång till uppgifter.