Sebastian Meglic
Säkerhets- och beredskapssamordnare
sebastian.meglic@trelleborg.se
0708-81 71 64

Kommunstyrelsen

Riktlinje för dataskydd – GDPR i Trelleborgs kommun och dess bolag

Innehållsförteckning

1. Inledning

Att värna den personliga integriteten för de personer vars personuppgifter behandlas i kommunens verksamheter är en viktig strategisk fråga för Trelleborgs kommun. I arbetet med personuppgiftsbehandling ska kommunen vara en bra part som arbetar förebyggande.

Personuppgifter ska alltid behandlas i enlighet med lagar och förordningar, bland annat EU:s dataskyddsförordning (GDPR).

Dataskyddsförordningen beskriver när personuppgifter får behandlas, med stöd av lag eller avtal, i myndighetsutövning eller med stöd av samtycke från de registrerade. Den är teknikoberoende och ska tillämpas på all behandling av personuppgifter, oavsett om behandlingen är teknisk eller manuell. Den som behandlar personuppgifter måste ha god kännedom om tillräckliga säkerhetsåtgärder för att uppgifterna skyddas på rätt sätt.

Ytterligare relevant lagstiftning kan tillkomma i form av exempelvis registerförfattningar inom specifika branschområden.

Inom ramen för Trelleborg Kommuns verksamhet är huvudsakligen följande lagar och bestämmelser relevanta:

- EU:s allmänna dataskyddsförordning
- den kompletterande svenska dataskyddslagen
- bokföringslagen
- arkivlagen
- lagen om elektronisk kommunikation
- offentlighets – och sekretesslagen
- kommunallagen och förvaltningslagen.

Notera att listan inte är uttömmande.

1.1. Begrepp och definitioner

Personuppgifter

En personuppgift är all information som kan användas för att identifiera en enskild levandes person, direkt eller indirekt. Begreppet personuppgifter inkluderar (men är inte begränsat till):

- namn
- personnummer
- e-postadress
- telefonnummer
- IP-adress
- kundnummer
- bilder och i vissa fall även ljudupptagningar.

Känslig personuppgift

I dataskyddsförordningen skiljer man mellan vanliga personuppgifter och känsliga personuppgifter. Normalt är det förbjudet att hantera känsliga personuppgifter,

men det finns undantag från förbudet. Känsliga uppgifter måste också skyddas mer än andra uppgifter.

Känsliga personuppgifter är uppgifter om:

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

Notera att även uppgifter som indirekt avslöjar känslig information av detta slag inkluderas som känsliga personuppgifter.

Behandling

Med behandling avses en åtgärd eller en kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller inte. Exempel på behandlingar är:

- insamling
- registrering
- lagring
- läsning
- användning
- utlämning genom överföring
- radering och förstöring.

Den registrerade

Fysiskt levande person som en personuppgift avser.

2. Grundläggande principer

I dataskyddsförordningen finns ett antal grundläggande principer som ska följas vid all behandling av personuppgifter. Det är den personuppgiftsansvariges ansvar att kunna visa att dessa principer har följts.

2.1. Laglighet

Laglighet innebär 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
- samtycke.

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. Se mer under rubrik *9. Rättsliga grunder för personuppgiftsbehandling.*

2.2. Korrekthet

Korrekthet 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.

2.3. 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.

2.4. 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 allt för 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.

2.5. 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.

2.6. 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.

2.7. 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.

2.8. Integritet och konfidentialitet

Personuppgiftsansvarig 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-virusskydd. Organisatoriska åtgärder handlar till exempel om interna rutiner, instruktioner och riktlinjer.

2.9. 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 dataskyddsombud.

3. Ansvar och roller

3.1. Vem är personuppgiftsansvarig?

Personuppgiftsansvarig är den organisation (till exempel aktiebolag, 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.

I Trelleborgs kommun är kommunstyrelsen och övriga nämnder personuppgiftsansvariga. **Ansvaret kan inte delegeras**.

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.

3.2. Innebörden i att vara personuppgiftsansvarig

Den personuppgiftsansvarige måste se till att all personuppgiftsbehandling sker i enlighet med dataskyddslagstiftningen. Den som är personuppgiftsansvarig kan överlåta den faktiska behandlingen av personuppgifter men personuppgiftsansvaret kan aldrig överlåtas.

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.

Personuppgiftansvaret är omfattande och listan nedan tjänar som vägledning men är inte uttömmande.

Personuppgiftsansvarig ansvarar bland annat för att

- all personuppgiftsbehandling alltid följer rådande dataskyddslagstiftning
- försäkra sig om att förvaltningen och verksamheten har en ändamålsenlig organisation med tillräckliga resurser och dokumenterad ansvarsfördelning
- upprätthålla registerförteckning över samtliga personuppgiftsbehandlingar i den ansvariges verksamhet
- säkerställa att medarbetarna har nödvändig kompetens för att kunna följa dataskyddslagstiftningen
- säkerställa att det tecknas personuppgiftsbiträdesavtal med de leverantörer och motsvarande som behandlar personuppgifter för verksamhetens räkning
- säkerställa att personuppgiftsincidenter hanteras i enlighet med lagstiftningens krav

- utse dataskyddsombud och anmäla dess kontaktuppgifter till tillsynsmyndigheten. Stödja dataskyddsombudet i utförandet av de uppgifter som dataskyddsförordningen föreskriver och se till att ombudet har tillräcklig kompetens.

3.3. Utnämning av dataskyddsombud

I dataskyddslagstiftningen ställs det krav på att alla myndigheter ska utse ett så kallat dataskyddsombud. Det innebär att kommunstyrelsen och varje nämnd utse måste utse ett dataskyddsombud. För kommunala bolag finns inget direkt krav på att utse ett dataskyddsombud med undantag för om man inom kärnverksamheten regelbundet, systematiskt och i stor omfattning övervakar enskilda personer eller om man inom kärnverksamheten behandlar känsliga personuppgifter eller uppgifter om brott i stor omfattning.

För att skapa god ordning i arbetet med personuppgifter och öka förtroendet hos de registrerade rekommenderas Trelleborgs kommuns kommunala bolag att utnämna ett skyddsombud oavsett om kraven är uppfyllda eller inte.

Anmälan till tillsynsmyndigheten av dataskyddsombudet 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 dataskyddsombud 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 dataskyddsombudets arbetsuppgifter ska kunna utföras på ett tillfredsställande sätt ska den personuppgiftsansvarige hålla dataskyddsombudet underrättad om vilka personuppgiftsbehandlingar som sker och de säkerhetsrutiner som skyddar personuppgifterna.

Personuppgiftsansvarig ska i god tid rådgöra med dataskyddsombudet 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, exempelvis kunder och media. Personuppgiftsansvarig ska stödja dataskyddsombudets arbete bland annat genom att ge denne tillgång till dokumentation och IT-system i den utsträckning som behövs.

3.4. Dataskyddsombud

Dataskyddsombudets arbetsuppgifter och ställning styrs av lagstiftning. Funktionen ska agera självständigt och får inte ta emot instruktioner eller bli föremål för sanktioner för att utfört sina arbetsuppgifter.

Vägledningen nedan utgör en del av dataskyddsombudets arbetsuppgifter men är inte uttömmande.

Som dataskyddsombud ska du

- informera och ge råd kring skyldigheter för personuppgiftsansvarige, personuppgiftsbiträdet och de anställda som behandlar personuppgifter
- bistå med dokumentation, mallar policy och riktlinjer, övervaka efterlevnad av GDPR samt ge information och utbilda personal
- på begäran ge råd vad gäller konsekvensbedömningen (DPIA) avseende dataskydd samt övervaka genomförandet
- samarbeta med tillsynsmyndigheten
- agera kontaktperson till de registrerade
- ta fram e-learning utbildning om dataskyddsförordningen som distribueras till kommunanställda
- sammankalla personuppgiftssamordnarna för kontinuerlig avstämning, ledning och stöttning genom GDPR styrgruppsmöten, fyra gånger per år.

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

3.5. Personuppgiftssamordnare

Personuppgiftssamordnare är en funktion som ska finnas på varje förvaltning och som utses av personuppgiftsansvarig. Rollen kan, om det är möjligt, kombineras med andra arbetsuppgifter.

Som personuppgiftssamordnare ska du stötta verksamhet, ledning och personuppgiftsansvarig genom lämpligtvis men inte uteslutande följande uppgifter:

- löpande uppdatera och följa upp registerförteckningen
- löpande följa upp att samtliga personuppgiftsbehandlingar analyseras i en risk- och konsekvensbedömning
- löpande följa upp att konsekvensbedömning avseende dataskydd (DPIA) genomförs i de fall lagstiftningen kräver detta
- administrera begäran om registerutdrag
- ge råd, stöd och påtala brister till verksamhetens ledning och berörd personal i frågor rörande dataskydd
- vara stöd vid upprättande av personuppgiftsbiträdesavtal
- hålla sig underrättad om utveckling av lagstiftningen och praxis inom området

- löpande följa upp att de kommunövergripande och förvaltningsspecifika rutinerna för hantering och anmälan av personuppgiftsincidenter är kända i verksamheten
- bidra till utvecklingen av kommungemensamma rutiner och arbetssätt
- föreslå förvaltningsspecifika rutiner och arbetsinstruktioner i de fall det behövs
- rådfråga och samråda med dataskyddsombudet för verksamhetens räkning
- vara dataskyddsombudets kontaktperson i dataskyddsfrågor samt delta i kommunens GDPR-styrgruppsmöten (fyra gånger per år).

3.6. Övriga chefer och medarbetare

Samtliga medarbetare har ett ansvar för att behandlingen av personuppgifter utförs på ett korrekt och lagligt sätt. Vid upptäckt av brister i dataskyddsarbetet ansvarar samtliga medarbetare för att rapportera detta till närmaste chef och/eller dataskyddsombud. Samtliga medarbetare har även ansvar för att genomföra och slutföra utskickade E-learning-utbildningar.

Riktlinjer, rutiner och andra styrdokument ska vara kända inom organisationen och det åligger varje chef att förmedla vikten av att följa gällande styrdokument.

Varje chef ska på uppmaning av dataskyddsombudet påminna sina anställda om att genomföra och slutföra utskickade E-learning-utbildningar.

4. Den registrerades rättigheter

Enligt dataskyddsförordningen har de registrerade ett antal rättigheter gentemot personuppgiftsansvarig. Flera av rättigheterna gäller i begränsad omfattning i offentlig förvaltning men framgår i sin helhet av 3 kap. artikel 12-23 Dataskyddsförordningen. Rutiner och arbetsbeskrivningar ska finnas tillgängligt på kommunens intranät (Trellnet) för att ge stöd i hur hanteringen av de registrerades rättigheter ska gå till.

4.1 Rätt till information

Alla vars personuppgifter hanteras av Trelleborg kommun har rätt till information om hur deras personuppgifter hanteras. Detta gäller såväl anställda som medborgare, kunder och andra grupper. Informationen ska vara lättillgänglig samt tillräckligt utförlig för att motsvara kraven i dataskyddslagstiftningen. Informationen ska lämnas på ett klart och tydligt sätt.

Informationen lämnas i huvudsak via intranätet (för anställda) och på den offentliga webbplatsen i form av en informationssida riktad till medborgare, kunder och användare.

4.2 Rätt till tillgång

Den registrerade har alltid rätt att begära tillgång till de personuppgifter som behandlas, bland annat i syfte att kontrollera att de är korrekta. Detta kallas också **rätt till registerutdrag**.

Begäran görs genom kontaktuppgifter förmedlade på hemsida och intranät. Den registrerade måste legitimera sig för att kunna begära registerutdrag. Legitimering gäller även vid utlämnande, se *Rutin – Begäran om registerutdrag KS 2021/924.*

4.3 Rätt till rättelse

Varje person har rätt att få felaktiga personuppgifter 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.

Om personuppgifter rättas på den enskildes begäran måste personuppgiftsansvarig också informera den som de har lämnat ut personuppgifterna till om att uppgifter rättats, om det inte är omöjligt eller innebär en alltför betungande insats. I samband med att en rättelse genomförts har personuppgiftsansvarig en skyldighet att se till att tidigare felaktiga uppgifter tas bort.

4.4 Rätt till radering

m den registrerade begär att bli bortglömd är personuppgiftsansvarig skyldig att radera personuppgifterna i vissa särskilda fall. Rätten att bli bortglömd är dock mycket begränsad i en offentlig verksamhet. Exempelvis kan det krävas att personuppgifterna sparas för att uppfylla lagstiftningens krav på bevarande av allmänna handlingar, för att kommunen ska kunna utföra en uppgift av allmänt intresse eller som ett led i kommunens myndighetsutövning.

Om personuppgifter raderas på den enskildes begäran måste personuppgiftsansvarige också informera den som de har lämnat ut personuppgifterna till om raderingen, om det inte är omöjligt eller innebär en alltför 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.

4.5 Övriga rättigheter

När behandling av personuppgifter sker via samtycke eller för att behandlingen är nödvändig för att fullgöra eller ingå avtal har den registrerade rätt att få en kopia av sina personuppgifter i ett vanligt förekommande maskinläsbart format (**rätt till dataportabilitet**).

De registrerade har i vissa fall rätt att kräva att behandlingen av personuppgifter begränsas (**rätt till begränsning av behandling)**, exempelvis under perioden som utredning sker vid begäran om rättelse.

Den registrerade kan lämna **klagomål** som avser behandling av personuppgifter till personuppgiftsansvarig, dataskyddsombudet eller tillsynsmyndigheten.

5. Personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har blivit förstörda, gått förlorade eller på annat sätt kommit i orätta händer genom exempelvis obehörig åtkomst eller obehörigt röjande. 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.

Det är personuppgiftsansvarig som ansvarar för att personuppgiftsincidenter hanteras, utreds, dokumenteras och anmäls korrekt.

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.

På kommunens intranät Trellnet finns rutiner och instruktioner för att anmäla, dokumentera, hantera och utreda personuppgiftsincidenter. På intranätet finns även länkar till e-tjänsten för att anmäla personuppgiftsincidenter.

5.2 Rapportera personuppgiftsincident

Rapportering av personuppgiftsincidenter ska ske i kommunens e-tjänst för personuppgiftsincidenter. Inrapporteringen ska analyseras kontinuerligt och åtgärder vidtas som en naturlig del i det skadeförebyggande arbetet. Alla incidenter ska rapporteras internt.

5.3 Anmälan till tillsynsmyndigheten

Beroende på hur allvarlig incidenten bedöms vara ska personuppgiftsincidenten anmälas vidare till Integritetsskyddsmyndigheten, IMY. Detta görs av verksamhetens dataskyddssamordnare i samråd med kommunens dataskyddsombud. Eventuell anmälan av incidenten till Integritetsskyddsmyndigheten ska ske inom 72 timmar från det att den upptäckts. Därför är det viktigt att anmäla en personuppgiftsincident skyndsamt.

5.4 Informera de registrerade

I vissa fall kan de registrerade behöva informeras om att en incident har inträffat. Detta kan bli aktuellt om det bedöms sannolikt att personuppgiftsincidenten leder till hög risk för fysiska personers rättigheter och frihet. Det är personuppgiftsansvarig som fattar beslut om den registrerade ska informeras i enlighet med delegationsordningen.

6. Risk- och konsekvensbedömningar (DPIA)

Alla personuppgiftsbehandlingar ska analyseras i en risk- och konsekvensbedömning. För detta arbete är förvaltningens personuppgiftssamordnare behjälplig. Analysen kräver att personuppgifterna 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 de registrerades rättigheter och friheter är den personuppgiftsansvarige skyldig att göra en konsekvensbedömning avseende dataskydd (DPIA) enligt bestämmelserna i artikel 35 dataskyddsförordningen. I dessa fall ska dataskyddsombudet rådfrågas och en konsekvensbedömning (DPIA) bokas in med ombudet.

7. Att tänka på vid upphandling

Innan inköp av system eller tjänster i vilka personuppgifter kommer att behandlas ska beställaren kartlägga, analysera och ställa krav så att lagstiftningen beaktas. Utgångspunkt för detta är den risk- och konsekvensbedömning som ska genomföras. Personuppgiftsbiträdesavtal ska alltid tecknas i de fall ett personuppgiftsbiträde anlitas.

Innan personuppgiftsbehandlingen påbörjas eller tekniska hjälpmedel köps in ska ändamålet med behandlingen samt den rättsliga grunden vara fastställd. Antalet uppgifter som behandlas ska inte vara fler än vad som är nödvändigt i förhållande till ändamålet, beställaren ska även säkerställa att uppgifterna som samlas in är korrekta.

Lagringsminimering ska tillämpas vilket innebär att personuppgifterna 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 dokumenthanteringsplan ska principen om lagringsminimering beaktas. Att ta bort uppgifter ska följa regler och rutiner för rensning och gallring.

För tekniska system där personuppgifter behandlas ska principerna om Dataskydd som standard och Inbyggt dataskydd beaktas. Dataskydd som standard (Privacy by default) innebär i korthet att den som behandlar personuppgifter ska se till att personuppgifter i standardfallet inte behandlas i onödan. Det kan till exempel handla om att de förvalda inställningarna i en tjänst är satta så att inte mer information än nödvändigt samlas in, delas ut eller visas. Inbyggt dataskydd (Privacy by design) innebär att hänsyn ska tas till integritetsskyddsreglerna redan när IT-system och rutiner utformas.

8. Personuppgifter i e-post

Dataskyddsförordningen omfattar även behandling av personuppgifter i ostrukturerad form vilket innebär att hantering av personuppgifter i e-post också räknas som en personuppgiftsbehandling och därav gäller samma krav som för övriga behandlingar.

Grundregeln för Trelleborgs kommun är att hantering av personuppgifter ska ske i system och inte i e-post. E-posten är inte heller en lämplig permanent lagringsyta och information ska i stället överföras till exempelvis ärendehanteringssystem och diariesystem.

Om personuppgifter ska skickas via e-post eller på annat sätt överföras digitalt ska uppgiften skyddas mot obehörig åtkomst, förändring och förstöring.

Mer information och rutiner kring e-posthantering och personuppgifter återfinns på intranätet Trellnet.

9. Rättsliga grunder för personuppgiftsbehandling

Vilka rättsliga grunder som gäller för behandling av personuppgifter framgår under rubrik 2.1.

Myndigheter och andra inom kommunal och offentlig verksamhet ska främst använda **avtal, rättslig förpliktelse** eller **myndighetsutövning** och **uppgift av allmänt intresse.**

Privata aktörer som är verksamma inom offentlig verksamhet, till exempel skolor eller hälso- och sjukvård som bedrivs i privat regi, 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.

9.1 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.

Uppgifter av allmänt intresse ska ha stöd i lag eller författning alternativt kollektivavtal eller beslut som har meddelats med stöd av lag eller annan författning.

Obligatoriska uppgifter som ålagts kommunen att utföra är av allmänt intresse. Kommunen har också stora möjligheter att göra frivilliga åtaganden som är av allmänt intresse som exempelvis bostäder, fritids- och idrottsanläggningar och åtgärder för att främja kommunens näringsliv och annan kulturell verksamhet.

9.2 Rättlig förpliktelse

Med rättslig förpliktelse menas att det finns lagar eller regler som gör att den personuppgiftsansvarige måste behandla vissa personuppgifter i sin 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 på situationer då rättslig förpliktelse kan var gällande:

a) Att inom hälso- och sjukvård föra journal.

b) Arbetsgivare är skyldig att redovisa skatter och sociala avgifter beträffande arbetstagarna.

c) Turordningsreglerna vid uppsägning av personal på grund av arbetsbrist gör att arbetsgivaren måste upprätta listor över anställda och lämna till facket.

9.3 Avtal

Ett avtal kan utgöra en rättslig grund för att behandla personuppgifter. Det krävs då 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. Det här gäller bara avtal som den registrerade har ingått eller planerar att ingå.

Exempel på situationer då avtal kan var gällande:

a) Arbetsgivare behandlar personuppgifter om en anställd för att kunna uppfylla anställningsavtalet för exempelvis löneberäkning, registrering av sjukfrånvaro eller i ett flextidsystem.

b) För att exempelvis kunna leverera varor/tjänster till kunder eller fakturera.

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.

9.4 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.

Tänk på följande innan rättsliga grunden samtycke väljs:

- **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 28 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 i stället inhämtas från den som har föräldraansvaret för barnet.

Exempel på situationer då samtycke kan användas:

a) En nämnd planerar vägarbeten. Nämnden erbjuder medborgarna 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. Medborgare som inte vill delta har inte gått miste om någon grundläggande service från myndigheten. Informationen finns även publikt på kommunens webbplats.

Exempel på situationer då samtycke **inte kan** användas:

b) En medborgare ansöker om en biståndsinsats. För att kunna hantera ansökan och komma fram till ett beslut måste vi behandla medborgarens personuppgifter. Vi agerar här som myndighet gentemot medborgaren och maktförhållandet mellan oss är väldigt ojämlikt. 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 i stället myndighetsutövning.

9.5 Grundläggande intresse

Denna rättsliga grund är ovanlig inom kommunal verksamhet och innebär att personuppgifter kan behandlas om det sker för att skydda den registrerades vitala intressen, alltså för att rädda liv. I huvudsak handlar det om tillfällen när den registrerade inte kan fatta beslut eller lämna samtycke, till exempel om en person är medvetslös. Om det går att lösa situationen på annat sätt, gör det. Det kanske till och med går att undvika att behandla personuppgifterna.

Exempel på situationer då grundläggande intresse kan var gällande:

a) 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.

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.

9.6 Intresseavvägning (kan inte användas av kommun)

Kan tillämpas när den personuppgiftsansvariges intresse att behandla en uppgift väger tyngre än den enskildes personliga integritet, när ändamålet för behandlingen rör ett berättigat intresse hos den personuppgiftsansvarige.

OBS! Intresseavvägning kan inte användas av myndigheter.

10. Rättsliga konsekvenser

Ansvaret för behandling av personuppgifter ligger alltid på den personuppgiftsansvarige. I Sverige är Integritetsskyddsmyndigheten (IMY).

10.1 Varning, reprimand eller föreläggande

Tillsynsmyndigheten kan utfärda varningar om en planerad behandling av personuppgifter sannolikt kommer att bryta mot bestämmelserna i dataskyddsförordningen. Myndigheten kan utfärda reprimander om en pågående behandling av personuppgifter bryter mot bestämmelserna och kan dessutom förelägga organisationen till exempel om att den måste upphöra med en viss personuppgiftsbehandling.

10.2 Administrativ sanktionsavgift

Tillsynsmyndigheten kan besluta att en myndighet som bryter mot reglerna i dataskyddsförordningen ska betala en administrativ sanktionsavgift. För offentliga myndigheter kan avgiften som mest vara tio miljoner kronor för allvarligare överträdelser. För de något mindre allvarliga överträdelserna gäller ett maxbelopp på fem miljoner kronor.

Hur hög sanktionsavgiften blir beror dels på vilken bestämmelse överträdelsen gäller, dels på omständigheterna i det enskilda fallet.

10.3 Skadestånd till registrerade

Varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av dataskyddsförordningen har rätt till ersättning från den personuppgiftsansvarige för den uppkomna skadan.

Bilagor

Följande dokument kopplade till denna riktlinje finns på intranätet Trellnet:

- Bilaga Rutin begäran av registerutdrag (KS 2021/924)
- Bilaga Rutin begäran om rättelse av felaktiga personuppgifter (KS 2021/924)
- Bilaga information till registrerade
- Bilaga Rutin - personuppgiftsincident (KS 2021/924)
- Bilaga hantering av personuppgifter i ostrukturerat material
- Bilaga konsekvensbedömning
- Bilaga för GDPR i digitala kanaler
- Bilaga Rutin e-posthantering (KS 2021/180).