Sävsjö kommun

Plan/Program
Strategi
Handlingsplan
Policy
>>Riktlinje<<
Regel/Föreskrift

Riktlinjer för behandling av personuppgifter

Antagen av Kommunstyrelsen 2019-05-21 § 230

Antagen: Kommunstyrelsen 2019-05-21 § 230
Dokumentansvarig: Personuppgiftssamordnare
Gäller för: För alla nämnder och förvaltningar
Ersätter tidigare styrdokument: Nej
Diarienummer: KS 2019/140.003

Dokumentet gäller tills vidare.

Innehåll

Inledning

Den allmänna dataskyddsförordningen (2016/679) trädde i kraft den 25 maj 2018 och reglerar både offentliga och privata organisationers behandling av personuppgifter. Till skillnad från ett direktiv utgör en förordning en bindande och tvingande rättsakt för unionens medlemmar. Syftet med dataskyddsförordningen är att samordna och modernisera medlemmarnas lagstiftning inom området för personuppgiftsbehandling och dataskydd (Europaparlamentets och rådets förordning, 2016/679).

Dataskyddsförordningen ersätter därmed Sveriges tidigare lagstiftning, personuppgiftslagen (1998:204) ofta förkortad PuL som även den baserades på EU-rätten fast i form av ett direktiv (dataskyddsdirektivet 95/46/EG).

Syfte

Syftet är att tillhandahålla kommunövergripande riktlinjer samt bidra till ökad förståelse för behandling av personuppgifter inom kommunen. Informationen i detta styrdokument regleras av den allmänna dataskyddsförordningen (2016/679) och därtill även dataskyddslagen (2018:218) som innehåller nationella kompletterande bestämmelser avseende dataskyddsförordningen.

Syftet är därmed att tillhandahålla instruktioner så att kommunen aktivt kan arbeta med att samordna och styra arbetet gällande dataskydd och personuppgiftsbehandling samt grundlägga incitament för interna rutiner på förvaltningarna.

Grundläggande begrepp och definitioner

Vad är en personuppgift?

Definitionen av begreppet personuppgift återfinns i artikel 4 i den allmänna dataskyddsförordningen (2016/679). En personuppgift är information som direkt eller indirekt kan hänföras till eller användas för att identifiera en levande person (fysisk person). Vanligt förekommande exempel på personuppgifter kan vara namn, adress och olika typer av identifikationsnummer i form av personnummer eller dossiernummer.

Även uppgifter som fastighetsbeteckning, telefonnummer, bilder (om individen tydligt kan urskiljas på bilden) och ljudupptagningar kan betraktas som personuppgifter. Avgörande är att uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en nu levande fysisk person.

Vad avser behandling av personuppgifter?

Behandling av personuppgifter avser alla åtgärder gällande personuppgifter, automatiserade eller ej, som utförs av en personuppgiftsansvarig. Det kan exempelvis handla om registrering, lagring och bearbetning av elevers personuppgifter i de verksamhetssystem som används för elevadministration. Ett annat exempel är att den anställde mottager e-post innehållandes personuppgifter, e-posten bör således snabbt raderas och uppgifterna överföras till säker lagringsplats, exempelvis ett verksamhetssystem.

Nedan följer exempel på vad som utgör behandling av personuppgifter:

- Insamling
- Registrering

- Lagring
- Bearbetning
- Ändring
- Läsning
- Överföring
- Radering/gallring

Vem är personuppgiftsansvarig?

Personuppgiftsansvarig är den organisation som innehar personuppgifter samt bestämmer ändamålen för behandlingen av personuppgifterna. En personuppgiftsansvarig kan således vara en fysisk eller juridisk person, offentlig myndighet, frivilligorganisation eller ett privat företag. Det är den personuppgiftsansvarige som innehar ansvaret för att behandlingen av personuppgifter sker i enlighet med dataskyddsförordningen. Kommunen är en geografisk enhet bestående av ett flertal myndigheter, det vill säga, kommunala organ med en självständig ställning. I Sävsjö kommun är därmed kommunstyrelsen, respektive nämnd, kommunalt bolag samt kommunfullmäktiges revisorer personuppgiftsansvariga för de behandlingar som utförs inom deras verksamhetsområden. De kommunala myndighetsgränserna reglerar således ansvarsfördelningen för personuppgiftsansvaret.

Om två eller flera organisationer gemensamt ansvarar för behandlingar av personuppgifter är de två organisationerna personuppgiftsansvariga tillsammans och ska inbördes fördela ansvaret för hur de ska fullgöra skyldigheterna som regleras i dataskyddsförordningen.

Personuppgiftsbiträde och personuppgiftsbiträdesavtal

Ett personuppgiftsbiträde är en extern aktör i form av en organisation eller en juridisk eller fysisk person som finns utanför den personuppgiftsansvariges organisation och som behandlar personuppgifter på uppdrag åt den personuppgiftsansvarige. Ett exempel på ett personuppgiftsbiträde är en leverantör för ett verksamhetssystem vars system används av den personuppgiftsansvarige för att behandla personuppgifter. Den personuppgiftsansvarige kan överlåta utförandet av behandling av personuppgifter men personuppgiftsansvaret kan aldrig överlåtas. De personuppgiftsbiträden som behandlar personuppgifter i uppdrag åt den personuppgiftsansvarige ska kunna garantera att behandlingen uppfyller kraven i dataskyddsförordningen. De skyldigheter som gäller för den personuppgiftsansvarige gäller även för personuppgiftsbiträdet. Även tillsyn från Datainspektionen eller skadeståndskrav kan drabba personuppgiftsbiträdet.

Ett avtal ska upprättas för att bekräfta att personuppgiftsbiträdet får behandla personuppgifter åt den ansvarige. Ett sådant avtal benämns som *personuppgiftsbiträdesavtal.* Ett personuppgiftsbiträde får enbart behandla personuppgifter enligt de instruktioner och bestämmelser som ingår i det personuppgiftsbiträdesavtal som upprättats. Respektive personuppgiftsansvarig ansvarar för att personuppgiftsbiträdesavtal upprättas med den externa aktören.

Personuppgiftsansvarig bör i så stor utsträckning som möjligt använda sig av det den mall för personuppgiftsbiträdesavtal som tagits fram av Sveriges kommuner och Landsting (SKL). Mallen ska finnas att tillgå på kommunens intranät under fliken ”Informationssäkerhet och GDPR.

Registerförteckning och hel- och delvis automatiserad behandling

Personuppgiftsansvariga myndigheter ska föra register över all behandling av personuppgifter som sker i deras verksamheter och som omfattas av dataskyddsförordningen. De behandlingar som omfattas av dataskyddsförordningen gäller för helt eller delvis digital behandling, kallad automatiserad behandling. En delvis automatiserad behandling kan vara när en verksamhet först samlar in personuppgifter manuellt för att sedan lagra uppgifterna i ett automatiserat register. Dataskyddsförordningen omfattar dock även manuell behandling, utan att en dator använts, då personuppgifterna 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[1].

För helt eller delvis automatiserad behandling gäller regelverket både personuppgifter som lagras i registerform och i ostrukturerad form. Det senare kan vara till exempel personuppgifter i ordbehandlingsdokument, på webbplatser eller i e-post[2].

Dataskyddsombud

Enligt dataskyddsförordningen, artikel 37 i Europaparlamentets och rådets förordning, 2016/679, är alla myndigheter och offentliga organisationer ålagda att ha ett dataskyddsombud som kontrollerar att myndigheten behandlar de registrerades personuppgifter i enlighet med dataskyddsförordningens krav och även verkar rådgivande gentemot personuppgiftsansvarige.

Det innebär att kommunstyrelsen, respektive nämnd och kommunrevisionen i egenskap av deras ställning som myndighet är skyldiga att utse ett dataskyddsombud som sker genom ett beslut från respektive instans.

Även kommunala bolag (hel- och majoritetsägda) omfattas av kravet på att utse dataskyddsombud. De är visserligen privaträttsliga organ men är upprättade med stöd av regler i kommunallagen (2017:725) och utför ”kommunala uppgifter”[3]. Dataskyddsombudet innehar en rapporteringsskyldighet till tillsynsmyndigheten Datainspektionen vid exempelvis personuppgiftsincidenter. Dataskyddsombudet verkar oberoende från den organisation som den bevakar.

Flertalet kommuner väljer att samordna finansieringen av tjänsten inom aktuellt kommunalförbund eller genom annat kommunalt samarbete då ett dataskyddsombud får verka gentemot flera organisationer. Sävsjö kommun, som är en del av kommunalförbundet Höglandsförbundet innehar ett gemensamt dataskyddsombud med de övriga höglandskommunerna.

Organisation och ansvarsfördelning

I den personuppgiftsansvariges ansvar ingår därmed att arbeta för att säkerhetsställa att varje behandling av personuppgifter som utförs har ett tydligt ändamål innan behandlingen påbörjas.

---

[1] https://www.datainspektionen.se/vagledningar/for-foreningar-och-sma-organisationer/det-har-behover-ni-veta/

[2] https://www.datainspektionen.se/vagledningar/for-foreningar-och-sma-organisationer/det-har-behover-ni-veta/

[3] En vägledning från SKL – Dataskyddsombud i kommun, landsting och regioner (2018)

Kortfattat kan nämndens eller styrelsens ansvar beskrivas i följande punkter:

1. Ansvar för att riktlinjerna i detta styrdokument följs,
2. Ansvar för att dataskyddsombud utses,
3. Ansvar för att rutiner för dataskydd upprätthålls gällande registerutdrag, rättning och gallring av personuppgifter,
4. Ansvar för att nya registreringar förtecknas och uppdateras med jämna mellanrum,
5. Ansvar för att garantera att organisatoriska resurser finns tillgängliga och fördelas,
6. Ansvar att personuppgiftsincident anmäls upprättas och skickas till Datainspektionen i samråd med dataskyddsombud och personuppgiftssamordnare,
7. Ansvar för samverkan med personuppgiftssamordnare på kommunledningskontoret gällande nya registreringar, uppfattade brister i verksamheten och övriga frågor som rör dataskydd och informationssäkerhet,
8. Ansvar för att tekniska resurser upprätthålls i samverkan med leverantör,

Personuppgiftssamordnare och övergripande arbete

Personuppgiftssamordnare utgör den centrala funktionen för kommunens arbete för behandling av personuppgifter. Personuppgiftssamordnare utgör även personuppgiftadministratör för kommunstyrelsen.

Personuppgiftssamordnare har till uppgift att utöva en övergripande tillsyn över kommunövergripande riktlinjer, utöva tillsyn över registerförteckningar, stödja förvaltningarna samt dess personuppgiftsadministratörer i interna rutiner i den mån som behövs samt samverka med dataskyddsombud och personuppgiftsadministratörer.

Personuppgiftsadministratörer

Respektive nämnd är ytterst ansvarig för den interna ansvarsfördelningen medan personuppgiftssamordnare fortsatt organiserar hur det samordnande arbetet ska ske på kommunövergripande nivå.

Förvaltningschef för respektive förvaltning bör därmed i samspråk med kommunens personuppgiftssamordnare utse en personuppgiftsadministratör, en representant från varje förvaltning, som samordnar och kontrollerar på nämndnivå samt återrapporterar till personuppgiftssamordnare om hur arbetet fortlöper eller om frågor uppstår. Vid behov utses även representanter från förvaltningens olika avdelningar om en förvaltning är omfattande eller har varierande verksamhetsområden.

Personuppgiftsadministratören ska även kunna rådgöra med personuppgiftssamordnare och dataskyddsombud.

Dataskyddsgrupp

Personuppgiftsadministratörer och personuppgiftssamordnare ingår därmed i kommunens dataskyddsgrupp som utgör samordnar och kontrollerar arbetet inom sina förvaltningar/avdelningar. Personuppgiftssamordnaren utgör kontaktperson gentemot dataskyddsombudet för kommunstyrelsen och kommunen i sin helhet medan personuppgiftsadministratörerna representerar sin nämnd.

Personuppgiftssamordnare sammankallar dataskyddsgruppen.

Principer för behandling av personuppgifter

Enligt artikel 5 i Europaparlamentets och rådets förordning, 2016/679 finns ett antal principer som personuppgiftsansvarig och personuppgiftsbiträden ska uppfylla vid behandling av de registrerades personuppgifter och listas här nedan:

Laglighet, korrekthet och öppenhet

Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Det innebär att den personuppgiftsansvarige måste hänvisa behandlingen av personuppgifter till en av de rättsliga grunderna som beskrivs i nästa avsnitt. Den registrerade ska få information om varför och hur deras personuppgifter behandlas, både innan behandlingen av personuppgifterna påbörjas samt när den registrerade begär vidare information.

Ändamålsbegränsning

Uppgifterna ska samlas in för tydliga och berättigade ändamål och får inte heller behandlas på ett sätt som är oförenligt med ändamålen. Ändamålet ska vara tydligt utformat redan innan uppgifterna insamlas. Personuppgifter får behandlas för arkiv- och forskningsändamål eller för annat vetenskapligt, historiskt eller statistiskt syfte om det inte anses oförenligt med det ursprungliga ändamålet.

Uppgiftsminimering

Åtgärder och uppgifter ska motsvara ändamålet för vilka de behandlas, alltså inte för omfattande i förhållande till det ursprungliga ändamålet. Om uppgifterna saknar relevans för dagens behandling så ska de gallras, sådan information bör även framgå av den dokumenthanteringsplan som fastställts av respektive organ.

Korrekthet

Uppgifterna ska vara korrekta och uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga raderas eller rättas utan dröjsmål.

Lagringsminimering

Uppgifterna får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Om den rättsliga grunden för en personuppgiftsbehandling inte längre är applicerbar, måste personuppgiften gallras, förutsatt att det inte finns några hinder för gallring i andra lagar.

Integritet och konfidentialitet

Uppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling, mot förlust förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

Ansvarsskyldighet

Den sista principen hänvisar till skyldighet för personuppgiftsansvarige och biträde att ovanstående principer följs.

Rättsliga grunder för behandling av personuppgifter

Enligt dataskyddsförordningen grundläggs sex rättsliga grunder som respektive personuppgiftsansvarig eller personuppgiftsbiträde måste uppfylla för att behandla personuppgifter. Det innebär att den personuppgiftsansvarige måste ha ett tydligt och avgränsat ändamål med sin behandling som ska grunda sig i någon av de rättsliga grunderna för att den ska vara laglig.

De rättsliga grunderna som offentlig verksamhet främst vilar på är ”uppgifter av allmänt intresse” och ”myndighetsutövning” men även ”rättslig förpliktelse”. Myndigheter och organ har dock blivit undantagna möjligheten att stödja en personuppgiftsbehandling på den rättsliga grunden ”intresseavvägning”. Myndighetsutövning, uppgift av allmänt intresse och rättslig förpliktelse innebär att myndigheten har rätt att utföra behandlingar som har stöd i aktuell lagstiftning och annan författning och är uppgifter som ålagts myndigheter att utföra.

Samtycke

Samtycke innebär att den registrerade har samtyckt till personuppgiftsbehandlingen. Den registrerade har dock rätt att ta tillbaka sitt samtycke till behandlingen. Samtycke kan dras tillbaka närsomhelst men gäller till och med den dag då återtagandet skedde. Behandlingen som personen redan har samtyckt till kan inte påverkas retroaktivt.

Observera att det i många fall inte är det inte lämpligt att den rättsliga grunden utgörs av den registrerades samtycke eftersom samtycket kan dras tillbaka och det kan vara svårt att bevisa att den registrerade har samtyckt, det ska i så fall ske skriftligt. Den personuppgiftsansvarige bör alltid överväga om man kan stödja personuppgiftsbehandlingen på någon av de andra rättsliga grunderna. Ibland kan samtycke utgöra det enda alternativet, exempelvis för insamling av samtycke för publicering av foton på kommunens webbplats.

Grundläggande intressen

Behandling av personuppgifter får i undantagsfall ske utan samtycke för att skydda en registrerad som inte kan lämna samtycke vid exempelvis sjukdom.

Avtal

Den registrerade kan även ingå ett avtal med den personuppgiftsansvarige om personuppgiftsbehandlingen. För att ingå avtal måste personen ha fyllt 18 år.

Rättslig förpliktelse

Den personuppgiftsansvarige kan vara rättsligt förpliktigad att följa de lagar, regler eller annan författning som ålägger personuppgiftsansvarige att utföra en viss personuppgiftsbehandling.

Myndighetsutövning och uppgift av allmänt intresse

Behandling av personuppgifter i samband med myndighetsutövning är en återkommande rättslig grund inom kommunal verksamhet. Begreppet myndighetsutövning har tagits bort i den reviderade förvaltningslagen som trädde i kraft 1 juli 2018 (2017:900) men kan beskrivas som ”utövande av makt i förhållande till enskild”. Uppgift av allmänt intresse innebär att myndigheten har rätt att utföra behandlingar som har stöd i aktuell och allmän lagstiftning.

Det kan ibland vara svårt att skilja på vad som är en ”uppgift av allmänt intresse” eller ”rättslig förpliktelse”, eftersom båda grunderna utgår ifrån att myndigheten behöver stöd i lagstiftning eller annan författning för att kunna behandla personuppgifterna. Skiljelinjen

kan härledas till vad som utgör allmän eller kompletterande lagstiftning då rättslig förpliktelse har sin grund i kompletterande bestämmelser till en allmän lagstiftning, exempelvis skollagen (2010:800).

Det finns även en skiljelinje mellan myndighetsutövning och uppgift av allmänt intresse. Behandling av personuppgifter inom skol- och utbildningsverksamheten kan till stor del hänvisa sin rättsliga grund till ”uppgifter av allmänt intresse” medan betygsättning och orosanmälningar är exempel på ”myndighetsutövning”.

Kategorier av uppgifter

Känsliga uppgifter

I likhet med den tidigare personuppgiftslagen (1998:204) betraktas vissa personuppgifter fortsatt som ”känsliga personuppgifter” beroende på uppgifternas innehåll och de möjliga konsekvenserna för integritetsskyddet om obehöriga får åtkomst till uppgifterna. Följande personuppgifter nedan klassificeras enligt dataskyddsförordningen som känsliga:

1. Etniskt ursprung
2. Religiös åskådning eller filosofisk övertygelse
3. Politisk åskådning
4. Facktillhörighet
5. Uppgifter rörande hälsotillstånd
6. Uppgifter om en persons sexualliv eller sexuell läggning
7. Genetiska uppgifter och biometriska uppgifter (exempelvis fingeravtryck, iris)
8. Lagöverträdelser

Känsliga personuppgifter ska generellt inte behandlas av myndigheter förutom i de fall då den anställde kan hänvisa till stöd i lagstiftning. En individs namn kan avslöja en individs etniska ursprung men det är själva klassificeringen av individens etniska ursprung och nationalitet som är känslig uppgift som inte får behandlas utan lagstöd. Det ska för myndigheten finnas ett tydligt och övertygande ändamål för att få tillåtelse att behandla känsliga uppgifter. Uppgifter om hälsotillstånd och patientuppgifter bedöms vara känsliga personuppgifter som får behandlas inom de ramar som hälso- och sjukvårdslagstiftningen i form av patientdatalagen (2008:355) och socialtjänstlagen (2001:453) anger. Känsliga uppgifter måste i detta fall behandlas för att myndigheten ska kunna tillgodose vård till medborgare.

Känsliga uppgifter måste skyddas extra väl så att inga obehöriga kan komma åt dem i det aktuella verksamhets- eller journalsystemet som används. Det är ej tillåtet att sprida känsliga personuppgifter per e-post. Känsliga personuppgifter ska inte blandas ihop med extra skyddsvärda uppgifter som utgörs av exempelvis personnummer som beskrivs nedan.

Extra skyddsvärda uppgifter

Extra skyddsvärda personuppgifter är personuppgifter som inte klassificeras som känsliga uppgifter men som ändå bedöms inneha ett tydligare skyddsvärde framför andra personuppgifter. Extra skyddsvärda uppgifter utgörs av exempelvis identifikationsnummer, värderingar av ens persons förmågor och provresultat. Ett typiskt exempel på en extra skyddsvärd uppgift är personnummer som har ett utbrett användningsområde i både offentlig och privat verksamhet i Sverige men som bör hanteras med varsamhet. Undvik att

skicka extra skyddsvärda uppgifter som exempelvis personnummer via e-post och för in personuppgifterna i aktuellt verksamhetssystem skyndsamt.

Lagring, gallring och arkiv

Personuppgifter ska i största utsträckning lagras i myndigheternas verksamhetssystem. Känsliga uppgifter eller andra uppgifter som är belagda med sekretess med stöd i lagstiftning ska alltid och endast lagras i verksamhetssystem som respektive myndighet ansvarar för.

Offentlighetsprincipen och utelämnande av allmän handling

Offentlighetsprincipen åsyftar allmänhetens och massmedias rätt till insyn av statens och kommunernas verksamheter med stöd samt rätten att ta del av allmänna handlingar som regleras i 2 kap. 1-2 §§ i Tryckfrihetsförordningen (1949:105). Rätten att ta del av allmänna handlingar begränsas om handlingarna innehåller uppgifter som är sekretessbelagda enligt offentlighets- och sekretesslagen (2009:400), OSL eller annan speciallagstiftning.

Rätten till transparens och insyn i offentlig verksamhet utgör omfattande principer som grundlägger förvaltningens agerande. Dataskyddsförordningen och dataskyddslagen bör därmed inte påverka rätten att ta del av allmänna handlingar som bedöms vara offentliga. Förordningen och dataskyddslagen kan dock påverka **sättet** om vilket allmänna handlingar lämnas ut, ingår extra skyddsvärda uppgifter som personnummer i en offentlig allmän handling så bör inte handlingen skickas ut per e-post eftersom detta inte uppfyller kraven på säker e-posthantering. Känsliga uppgifter ska aldrig spridas i ett e-postmeddelande då det skulle leda till obehörig åtkomst.

En handling bedöms som allmän när den har inkommit eller upprättats hos en myndighet samt om den förvaras hos myndigheten enligt tryckfrihetsförordningen, 2 kap. 3 §, 6-7 §§. Det innebär att en handling kan bedömas som allmän när den korsar en myndighetsgräns och därmed lämnar den tidigare myndigheten och inkommer till en ny myndighet. Med myndigheter avses kommunstyrelsen och övriga nämnder, kommunfullmäktiges revisorer samt andra kommunala organ med självständig ställning medan kommunen utgör en geografisk enhet. Bestämmelserna gällande vad som anses vara en allmän handling utgår därmed ifrån myndighetsgränser.

Lagringsminimering, dokumenthantering och gallring

En annan lagstiftning är arkivlagen (1990:782) som reglerar myndigheters skyldighet att bevara allmänna handlingar och vidta de åtgärder som krävs för detta ändamål. Arkivlagen ålägger därmed myndigheter att bevara vissa allmänna handlingar för att säkerhetsställa att allmänheten får tillgång till dem. Vissa handlingar kommer därmed inte att få gallras, det gäller exempelvis protokoll från politiska sammanträden, elevvårdsjournaler, slutbetyg och barnplaceringsakter. I enlighet med Sävsjö kommuns arkivreglemente är därmed kommunstyrelsen, kommunfullmäktiges revisorer, respektive nämnd och kommunalt bolag inom Sävsjö kommun ålagd att upprätta en informations- och dokumenthanteringsplan som beskriver de förekommande handlingstyperna i myndighetens verksamheter och hur dessa hanteras. En bredare term är informationshanteringsplan då offentlig verksamhet idag hanterar olika former av information och inte endast fysiska eller digitala dokument. En dokument- och informationshanteringsplan utgör då även gallringsbeslut och reglerar då bestämmelserna kring gallring eller bevarande av myndighetens information.

Principen om lagringsminimering innebär att uppgifterna inte får lagras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Om en personuppgift inte längre är relevant för det ändamål som den en gång behandlades för så ska den gallras. För att säkerställa att personuppgifter inte sparas längre än nödvändigt bör det av registerförteckningen tydligt framgå hur länge personuppgifter ska lagras samt vilka rutiner som gäller för gallring.

Personuppgifter får dock lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Myndighetens verksamheter bör då kunna söka stöd i dokumenthanteringsplanen samt i aktuell lagstiftning som reglerar hur länge en uppgift får sparas eller i fall uppgiften ska bevaras och därmed arkiveras. Dokumenthanteringsplanen ska utgöra ett stöd för verksamheten för att snabbt få en uppfattning om vad verksamheten arbetar med för typ av information och hur den ska hanteras.

Hantering av bilder

För bilder, både stillbilder och filmer gäller dataskyddsförordningens regler om personerna direkt eller indirekt kan identifieras på bilderna, om ansiktet syns eller identifierande faktorer finns. För att få publicera bilder med personuppgifter behöver personuppgiftsansvarig knyta sin behandling till en relevant rättslig grund; myndighetsutövning och uppgift av allmänt intresse och samtycke är rättsliga grunder som kan knytas till hantering av bilder som innehåller personuppgifter.

E-post och ostrukturerad data

Dataskyddsförordningen och dataskyddslagen genererar krav på hur anställda och förtroendevalda inom offentlig verksamhet hanterar sin e-post. Inkommen e-post ska behandlas som traditionell pappershantering vad avser diarieföring och sekretess tills digitala verktyg anses tillräckliga för att ersätta dem. Samma regler för när en handling anses vara inkommen och upprättad appliceras även på e-post. När en e-post skickas från en nämnd till en annan nämnd så kan den bedömas utgöra en allmän handling då den har korsat myndighetsgränsen. Om handlingen istället skickas mellan nämndens olika avdelningar så lämnar den inte myndigheten.

En grundregel är att hålla privata konversationer utanför kommunala e-postkonton och kommunalägd teknisk utrustning oavsett om informationsutbytet sker inom en nämnd eller inte, privat e-post som ändå inkommit bör rensas från e-postlådan. I all kommunal e-post ingår någon form av information som kan hänvisas till en individ exempelvis namnet på det anställde framgår i den kommunala e-postadressen och därmed omfattas e-posten av dataskyddsförordningen.

Postlista och e-postloggar utgör en offentlig allmän handling.

Känsliga personuppgifter ska endast behandlas i de fall som den anställde kan hänvisa till stöd i nuvarande lagstiftning. Känsliga uppgifter får inte spridas via e-post, varken internt inom myndigheten eller mellan olika myndigheter.

Riktlinjer för kommunal e-posthantering

Att tänka på när man som kommunanställd använder sin kommunala e-postadress:

1. Om du är frånvarande från din tjänst under en längre period; exempelvis vid semestertider så krävs en fullmakt för att en annan medarbetare ska vara ombud för din personliga kommunala e-postadress.

2. Om du inte har möjlighet att svara på e-posten eller den fråga som ställs så kan du meddela att du har mottagit e-postmeddelandet och be att få återkomma med konkret svar eller besked snarast möjligt.

3. Informera via autosvar om frånvaro och hänvisa även till annan medarbetare, exempelvis din chef.

4. Ett e-postmeddelande med personuppgifter får inte ligga kvar i inkorgen eller i skickat-mappen hur lång tid som helst. När din behandling av personuppgifter är klar ska informationen antingen flyttas över till lämpligt system eller raderas från e-postinkorgen. Lagring av personuppgifter i e-post ska begränsas/undvikas. Om en anställd till exempel sjukanmäler sig via e-post: registrera det i systemet och radera e-posten.

5. Sprid inte personuppgifter i onödan utanför verksamhetssystem. Om någon annan anställd behöver ha tillgång till vissa uppgifter för att kunna utföra en arbetsuppgift, överväg istället telefonsamtal eller andra sätt.

6. Skicka ej *extra skyddsvärda uppgifter* som exempelvis personnummer, värderingar av en persons förmåga eller provresultat via e-post.

7. Om du måste använda e-post, se över om det går att avidentifiera uppgifterna.

8. Undvik att skicka massutskick till större e-postgrupper. Använd funktionen hemlig kopia om e-post ska skickas till ett stort antal personer.

Den registrerades rättigheter

Allmän information till den registrerade

Enligt dataskyddsförordningen har den registrerade rätt att få information om hur dennes personuppgifter behandlas. Informera därmed alltid den registrerade om hur uppgifterna ska användas innan en insamling av uppgifter påbörjas. Informera annars i samband med att myndigheten utför behandlingen om uppgifterna hämtas från exempelvis annan myndighet. Information bör ges i skriftlig form för att säkerhetsställa att informationen har delgetts de registrerade samt på grund av krav på tydlighet och lättillgänglighet i dataskyddsförordningen. Om insamling av uppgifter sker genom en blankett så bör informationen vara med på blanketten.

På kommunens webbplats ska den registrerade kunna få allmän information om personuppgiftsansvarigas behandling av personuppgifter. Informationen ska enligt dataskyddsförordningen även vara lättillgänglig så informationen bör finnas tillgänglig på webbplatsens startsida och genom direktlänkar.

Enligt dataskyddsförordningen så måste en begäran av information följas av rimlighet för att den personuppgiftsansvarige ska kunna svara på den. Om en begäran skulle resultera i en alltför stor arbetsinsats eller att det är omöjligt att svara på den så har personuppgiftsansvarige rätt att avslå begäran via ett delegationsbeslut.

Information till den registrerade om behandling av personuppgifter

Följande information nedan ska delges en registrerad. Den registrerade har även rätt att få information om det skett en personuppgiftsincident hos den personuppgiftsansvarige som påverkat personuppgifterna.

1. **Personuppgiftsansvarig**

Ange vilken myndighet/organ som är personuppgiftsansvarig för behandlingen och vem som samlar in informationen. Ange om det rör personen i egenskap av vårdnadshavare, elev, brukare, klient, medborgare eller anställd. Röd text kan tas bort om det inte är aktuellt.

Sävsjö kommun avser att genomföra en personuppgiftsbehandling som rör dig och ditt minderåriga barn. Kommunstyrelsen/nämnden är personuppgiftsansvarig för behandlingen av dina personuppgifter. Informationen samlas in av avdelning/förvaltning.

Personuppgiftsbehandlingen rör dig i egenskap av…

2. **Ändamålet med behandlingen,**

Ange ändamålet med behandlingen av personuppgifter; svara på frågan varför ni måste behandla personuppgifter till den registrerade.

Personuppgifterna behandlas för att…

3. **Kategorier av personuppgifter**

De kategorier av personuppgifter som ska lämnas av den registrerade exempelvis namn, telefonnummer och adress.

De kategorier av personuppgifter om dig som behandlas är…

4. Rättslig grund

Vilken som är utgör den rättsliga grunden för behandlingen:

- *Uppgift av allmänt intresse*
- *Myndighetsutövning*
- *Rättslig förpliktelse*
- *Avtal*
- *Samtycke*
- *Grundläggande intresse*

Den rättsliga grunden för personuppgiftsbehandlingen är…

5. Lagring/gallring

Den period under vilken personuppgifterna kommer att lagras och om de gallras eller arkiveras och därmed förvaras för all framtid. Ange hur länge uppgifterna lagras och vilka kriterier som gäller för gallring.

Uppgifterna om dig lagras..

6. Mottagare

De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, exempelvis vilka inom kommunen som informationen delas med.

De uppgifter som finns registrerade i det här fallet om dig kan komma att lämnas ut till… Personuppgifterna kommer inte att föras över till tredje land.

7. Kontaktuppgifter till kommunen och den registrerades rättigheter

Ange kontaktinformation. Kontaktinformationen som lämnas ut bör vara kommunens adress eller e-postadress, därmed kan den inkomna e-posten eller posten fördelas till rätt personuppgiftsansvarig när den väl inkommit.

Beskriv även kortfattat den registrerades rättigheter såsom rätten att bli glömd eller registerutdrag.

Du har rätt att kontakta Sävsjö kommun för att få information om vilka uppgifter om dig eller ditt minderåriga barn som finns registrerade. Du har också rätt att begära att få felaktiga uppgifter rättade, i vissa fall raderade eller begära att vi begränsar behandlingen. Det gör du genom att kontakta Sävsjö kommuns växel på telefonnummer 0382-152 00 eller mejl kommun@savsjo.se. Sävsjö kommuns dataskyddsombud nås via Höglandsförbundet, telefon 0380-51 75 19 eller mejladress dataskyddsombud@hoglandet.se. Mer information om dataskyddsombudet finns på Höglandsförbundets webbplats www.hoglandet.se.

8. Vid samtycke

Om den rättsliga grunden bygger på annat än samtycke hoppar du över denna punkt.

Du har rätt att när som helst ta tillbaka ditt samtycke. Detta gör du genom att kontakta kommunen på telefonnummer 0382-152 00 eller via mejl kommun@savsjo.se

9. Rätten att klaga till Datainspektionen

Ange rätten att framföra klagomål till tillsynsmyndigheten Datainspektionen.

Du har rätt att lämna klagomål till tillsynsmyndigheten Datainspektionen om du tycker att personuppgiftsansvarig behandlar dina personuppgifter på ett felaktigt sätt.

Den registrerades rättigheter

Rätt till rättelse

Den registrerade har rätt att begära att personuppgiftsansvarige rättar felaktiga personuppgifter eller uppdaterar informationen med relevanta uppgifter. Den som samlar in uppgifterna bör se till att de är korrekta.

Rätt till radering/rätten att bli glömd

Den registrerade har rätt att i vissa fall få sina personuppgifter raderade. Undantag gäller om uppgifterna används för att utföra en uppgift av allmänt intresse eller myndighetsutövning. Uppgifter kan ej raderas om uppgiften ska bevaras med stöd av offentlighetsprincipen eller aktuell lagstiftning som arkivlagen då arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål ej får gallras.

Uppgifterna ska raderas om:

1. Om uppgifterna inte längre är relevanta för de ändamål som de från början samlades eller behandlades för,

2. Om den rättsliga grunden för personuppgiftsbehandlingen har varit samtycke och den registrerade drar tillbaka sitt samtycke,

3. Om personuppgifterna inte har behandlats enligt vad dataskyddsförordning eller annan lagstiftning stipulerar,

4. Om radering krävs för att uppfylla en rättslig skyldighet,

Rätt till begränsning av behandling

I vissa fall har även den registrerade rätten att begära att behandlingen av registrerades personuppgifter begränsas. Personuppgifterna får därmed endast behandlas enligt vissa specifika syften som den registrerade därmed har godkänt. Inaktuella personuppgifter bör därmed begränsas tills de har rättats.

Registerutdrag

Enligt dataskyddsförordningen har den registrerade rätt att få ta del av information om dennes personuppgiftsbehandlingar som utförs av personuppgiftsansvarig. Personuppgiftsansvarig är därmed skyldig att lämna ut informationen till den registrerade genom ett så kallat registerutdrag.

Ett registerutdrag inkluderar både strukturerad och ostrukturerad data, ostrukturerad data kan finnas i stödprocesser i form av e-post, ordbehandlingsprogram, kalkylblad (Excel), enklare listor etcetera.

Ett registerutdrag ska innehålla:

1. Ändamål med behandlingen.

2. De kategorier av personuppgifter som behandlingen gäller,
3. De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut,
4. Om möjligt, den förutsedda period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period,
5. Förekomsten av rätten för personuppgiftsansvarig att begära rättelse eller radering av personuppgifterna. Även förekomsten av rätten till begränsning av behandling av personuppgifter som rör den registrerade bör omnämnas om de finns.
6. Rätten att inge klagomål till Datainspektionen,
7. Om personuppgifterna inte samlas in från den registrerade, all tillgänglig information om varifrån dessa uppgifter kommer,

Personuppgiftsincident

En personuppgiftsincident kan beskrivas som att det har inträffat eller att man misstänker att det skett en säkerhetsincident som har lett till att obehörig har tagit del av personuppgifter. Om medarbetare ser brister eller risker som kan leda till ett utfall av incident så ska det också anmälas.

1. Det kan exempelvis handla om att obehörig har tagit sig in ett av personuppgiftsansvarig eller biträdes verksamhetssystem där man lagrar personuppgifter.
2. Utskrift med känsliga personuppgifter har glömts kvar i skrivare.
3. Personuppgiftsansvarige eller biträde har utsatts för en cyberattack, belastning eller en dator har fått en skadlig kod som gör att obehörig kan komma åt personuppgifter.

Hur ska en personuppgiftsincident rapporteras?

Datainspektionen kräver att en personuppgiftsincident rapporteras inom 72 timmar från det att personuppgiftsincidenten upptäcktes. En ansökan måste därmed alltid rapporteras inom 72 timmar och det gäller även om hela incidenten inte är utredd eller att alla åtgärder inte är på plats än. Om personuppgiftsansvarig inte utreder hela incidenteten inom 72 timmar så ska Datainspektionen informeras om att en komplett incidentrapport kommer så snart som möjligt.

Avslutning

Checklista vid behandling av personuppgifter

Sammanfattningsvis för innehållet i det här styrdokumentet så finns en checklista från Datainspektionen som förvaltningarna kan utgå ifrån för att bedöma om och hur man når upp till principerna i dataskyddsförordningen:

1. **Bestäm ändamålet**: Varför ska ni behandla personuppgifter? Vad är ert syfte?
2. **Hitta en rättslig grund**: Vilken rättslig grund i dataskyddsförordningen stödjer ni er på när ni behandlar personuppgifter?
3. **Informera de registrerade:** Är informationen lätt att hitta och är den lätt att förstå för de registrerade?
4. **Ha rätt uppgifter:** Behandlar ni bara de personuppgifter som ni behöver för ändamålet? Har ni för mycket personuppgifter?
5. **Skydda personuppgifterna:** Har ni vidtagit tillräckliga tekniska och organisatoriska säkerhetsåtgärder? Har ni gjort en risk- och sårbarhetsanalys för känsliga och extra skyddsvärda uppgifter?
6. **Radera uppgifter:** Har ni rutiner för att radera personuppgifter när de inte längre behövs för ändamålet?
7. **Visa att ni gör rätt:** Har ni dokumenterat er personuppgiftsbehandling, inklusive beslut och överväganden? Har ni skapat interna riktlinjer för dataskydd och hantering av personuppgifter?