



Riktlinjer för personuppgiftshantering

Socialnämnden

Inledning – ny lagstiftning

Den 25 maj 2018 träder den nya dataskyddsförordningen (GDPR) i kraft. Förutom tydligare ansvarsfördelning när det gäller personuppgiftshantering i företag, myndigheter och andra juridiska person såsom t.ex. föreningar, är det framförallt ny lagstiftning som säkerställer den registrerades rättigheter som införs.

Då varje nämnd är personuppgiftsansvarig är det upp till varje nämnd att ta fram riktlinjer för sin personuppgiftshantering. Detta dokument innehåller även riktlinjer som är gemensamma för samtliga kommunens nämnder som bland annat behandlar kommungemensamma utgångspunkter i personuppgiftshantering, gemensamma system och hur vi ser på den registrerades rättigheter.

I slutet av dokumentet finns också gemensamma definitioner av exempelvis personuppgift, personuppgiftsansvarig och personuppgiftsbiträde.

Gemensamma riktlinjer

Kommunens behandling av personuppgifter

Kommunens utgångspunkt är att kommunen bara ska samla in personuppgifter i den omfattning som krävs för att kunna ha en rättssäker myndighetsutövning och att kunna bedriva den verksamhet som medborgarna och staten ålagt kommunen.

De allra flesta personuppgifter som kommunen samlar in och behandlar är nödvändiga för att kunna bedriva verksamhet och för att kunna fatta beslut i ärenden. Det förekommer dock att kommunen samlar in och behandlar uppgifter som en service åt våra kommuninnevånare. Dessa kräver samtycke från de vars personuppgifter hämtas in.

Vem är personuppgiftsansvarig och för vad?

I kommunens reglemente för Kommunstyrelsen, nämnder och beredningar fastställs att varje nämnd är personuppgiftsansvarig, vilket innebär att varje nämnd är personuppgiftsansvarig för de personuppgifter som nämnden eller kommunstyrelsen själv ensamt förfogar över. För personuppgifter som



delas mellan nämnderna gäller en i reglementet fastställd ansvarsfördelning vilket i huvudsak följer indelningen i verksamhetsansvar.

För de kommungemensamma systemen är det Kommunstyrelsen som ansvarar. Kommunstyrelsen ansvarar därmed för personuppgifter i kommungemensamma system såsom e-post, telefoni och arkiv samt personuppgifter relaterade till HR och all kommunens personal samt avlönade uppdragstagare och förtroendevalda. Kommunstyrelsen ansvarar även för personuppgifter i register över kunder och leverantörer samt för bilder som publiceras externt.

När gemensamma personuppgifter hanteras så ska dessa behandlas med samma varsamhet och enligt samma föreskrifter som gäller den egna förvaltningen.

Vem får teckna personuppgiftsbiträdesavtal?

Det är den nämnd som är personuppgiftsansvarig för kategorin av personuppgifter som ansvarar för att teckna avtal med extern part som behandlar personuppgifter, så kallat personuppgiftsbiträdesavtal.

Om personuppgiftsbiträdesavtalet är kopplat till ett leverantörsavtal tecknas det av den som har teckningsrätt. Om avtalet inte är förknippat med ett avtal eller är av mer generell karaktär så tecknas det som ett generellt avtal enligt gällande delegationsordning för nämnden. Observera att avtal inte kan tecknas av dataskyddsombud.

Kommungemensamma system

E-post

Kommunstyrelsen är personuppgiftsansvarig för e-posten. Känsliga personuppgifter ska inte mailas alls (och inte heller sparas), om det inte finns synnerliga skäl för detta. Grundregeln är att e-posten **inte** ska utgöra ett arkiv och ska gallras precis som övriga dokument enligt dokumenthanteringsplanerna. De dokument som ska bevaras ska bevaras i akt eller i verksamhets- ärendehanteringssystem. Övriga mail, som inte gäller aktuella ärenden, får sparas i maximalt 6 månader.

Intranät och hemsida

Respektive förvaltning är ansvarig för sin information på hemsidan och intranätet. Kommunstyrelsen är personuppgiftsansvarig för bilder som publiceras. Till dessa ska samtycke eller modellavtal finnas om det går att identifiera personen på bilden.



Mobiltelefoni

Kommunstyrelsen är personuppgiftsansvarig för information som lagras i telefoner som tillhandahålls av kommunen som arbetsgivare och som relateras till kommunens verksamheter. Grundregeln är att telefonen på samma sätt som e-post **inte** ska utgöra ett arkiv. Detta gäller såväl meddelandekonversationer som telefonbok. Inaktuella kontakter ska raderas från telefonboken.

Rätten att bli bortglömd (raderas) eller få rättelse

Då kommunen lyder under lagstiftningar som påverkar vad kommunen måste spara i form av Tryckfrihetsförordning, Offentlighets- och sekretesslag, Förvaltningslag och diverse speciallagstiftningar, där kommunen sparar informationen dels på grund av myndighetsutövningen med också allmänt intresse, så är det få uppgifter som ur den aspekten kan raderas.

Kommunen samlar in ett fåtal uppgifter på annan grund, exempelvis samtycke, och det handlar framförallt om frivilliga åtaganden exempelvis näringslivsregister och föreningsregister. Om det förekommer personuppgifter i dessa ska dessa raderas på begäran av den enskilda. Uppgifter som finns i kommunens system kan rättas på begäran av den enskilde om kommunen och den enskilde så är överens.

Begäran om radering eller rättelse lämnas i första hand till ansvarig nämnds myndighetsbrevlåda. Observera att själva begäran om rätten om radering eller rättelse i sig blir en allmän handling. Beslutet på begäran om radering eller rättelse ska vara skriftligt och innehålla besvärshänvisning.

Utlämnande av allmän handling är undantaget föreskrifterna i dataskyddsförordningen, så inget samtycke krävs för att lämna ut en handling med personuppgifter, under förutsättning att den inte omfattas av sekretess.

Rätten att se sina uppgifter

Den registrerade har rätten att en gång per år kostnadsfritt få se alla sina personuppgifter som den personuppgiftsansvarige har i sina register. En begäran skall hanteras inom 30 dagar. Dokument där andra personuppgifter förekommer ska maskeras.

Det är den personuppgiftsansvariga som avgör i vilket format personuppgifter lämnas. Söderköpings kommun lämnar företrädesvis ut uppgifter i pappersform i en särskilt upprättad mall. Begäran om rätten att få se sina uppgifter diarieförs och ska komma från den registrerade. För att



få se uppgifterna ska dessa hämtas i kommunhuset mot uppvisande av legitimation eller skickas via rekommenderad post.

Den enskilde kan begära ut sina data i elektronisk form för överföring till annan tjänst, så kallad portabilitet. Portabiliteten gäller dock endast uppgifter som med samtycke och som den enskilde själv har lämnat, och blir därför i väldigt begränsad omfattning aktuell i Söderköpings kommun.

Personuppgiftsincident

Den medarbetare som upptäcker personuppgiftsincident fyller i en anmälan på intranät/Kanal. Underlaget skickas sedan till kommunens GDPR-samordnare som i sin tur avgör om ytterligare åtgärder behöver vidtas och skickar sedan anmälan till tillsynsmyndighet.

En incident ska anmälas inom 48 timmar efter att incidenten upptäcktes. Anmälan skickas till tillsynsmyndighet senast 72 timmar efter att incidenten upptäcktes.

Kommunens GDPR-samordnare ansvarar även för att information till den registrerade vid personuppgiftsincident sker enligt förordningen.

Gemensamma definitioner

Personuppgift

Varje upplysning som avser en identifierad eller identifierbar fysisk person (registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringssuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet. En bild kan också vara en personuppgift.

Känsliga personuppgifter

Med känsliga personuppgifter avses uppgifter om ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter som entydigt identifierar en person.

Behandling

Åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.



Personuppgiftsansvarig

Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. I Söderköpings kommuns fall respektive nämnd.

Personuppgiftsbiträde

Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Personuppgiftsincident

En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. Detta kan gälla såväl olovlig åtkomst till datasystem som till uppgifter i pappersform. Förlust av ett nedskrivet lösenord som går att använda till att se personuppgifter är en incident.

Dataskyddsombud

Myndigheter som behandlar personuppgifter måste utse ett dataskyddsombud. Ombudets roll är att kontrollera att dataskyddsförordningen följs inom organisationen genom att till exempel utföra kontroller och informationsinsatser.

Nämndens riktlinjer i övrigt

Användande av digitala tjänster och programvara

I socialnämndens verksamheter får bara användas programvara och tjänster där det finns tecknat personuppgiftsbiträdesavtal, om det finns minsta risk för att personuppgifter hanteras på ett otillbörligt sätt ska leverantören bytas.

Inga bilder eller andra känsliga personuppgifter får lagras i molnet, vilket innebär att bilder på verksamheten inte får tas med telefon eller surfplatta kopplat till exempelvis iCloud.

Hantering av material i pappersform

Utskrifter från register med personuppgifter omfattas även av GDPR. Det innebär att exempelvis listor för olika aktiviteter inom socialförvaltningen ska hanteras i enlighet med Socialnämndens fastställda dokumenthanteringsplan.