Bilaga 1: Riktlinje för behandling av personuppgifter

Denna riktlinje är en bilaga till Policyn för behandling av personuppgifter för Surahammars kommun och dess bolag fastställd av kommunfullmäktige 2018-05-28.

Strukturerad behandling

Inom Surahammars kommun och dess bolag ska samtliga behandlingar av personuppgifter registreras i respektive nämnds registerförteckning. Verksamhetens Dataskyddssamordnare granskar, med stöd av Dataskyddsombudet, om behandlingen har rättslig grund utifrån principerna för behandling av personuppgifter, som myndighet används följande rättsliga grunder:

1. Samtycke, används i undantagsfall då ingen annan rättslig grund kan användas
2. Avtal
3. Rättslig förpliktelse
4. Uppgift av allmänt intresse eller myndighetsutövning

Personuppgifterna får inte senare behandlas på ett sätt som är oförenligt med det initiala ändamålet och inte heller sparas längre än nödvändigt. Den som behandlar personuppgifter ska kunna visa att principerna följs.

Ostrukturerad behandling

Ostrukturerad behandling definieras som sådan behandling av personuppgifter som inte ingår i, eller är avsedda att ingå i, en samling av personuppgifter som har strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter. Typexempel är behandling av personuppgifter i löpande text i ordbehandlingsprogram, löpande text på internet, ljud- och bildupptagningar och e-post. Enkla listor är också exempel på ostrukturerat material. Detta innebär att samma regler gäller för alla personuppgifter.

Kravet på registrering omfattar både personuppgifter i separata program/system och register/listor som upprättas i andra program, så som Microsoft Excel, Word, och som bevaras i filformat.

Hantering av personuppgifter ska främst, och så långt det är möjligt, ske i gemensamma program/system.

E-post

Hantering av personuppgifter i e-post räknas som behandling av personuppgifter och har samma krav som andra behandlingar. Avseende rättslig grund faller e-post inom flera principer. Huvudparten kan dock hänföras till ”Uppgifter av allmänt intresse”, ”myndighetsutövning” samt ”Rättslig förpliktelse” vid speciallagstiftning.

E-post med personuppgifter ska inte ligga kvar i inkorgen eller i skickat mappen hur lång tid som helst. När behandlingen av personuppgiften är klar ska informationen flyttas över till lämpligt program/system och e-postmeddelandet raderas. Den tid som personuppgiften lagras i e-post ska begränsas till ett minimum. Det åvilar både avsändare och mottagare av e-post att uppmärksamma detta.

I e-post ska inte personuppgifter som är känsliga eller sekretessbelagda behandlas. Med känsliga personuppgifter avses etnicitet, genetik, hälsa, sexualliv och sexuell läggning samt politisk, facklig, filosofisk och religiös övertygelse. **E-post som sker genom särskild hantering med högre och tillräckligt hög säkerhetsnivå, till exempel kryptering, kan i vissa fall även behandla känsliga eller sekretessbelagda uppgifter.**

Information till registrerade

Den registrerade ska få tydlig information kring kommunens och bolagens behandling av personuppgifter. Den registrerade ska få information om behandlingen den omfattas av samt de rättigheter den har enligt gällande lagstiftning. Exempel på information som ska ges till den registrerade är den lagliga grunden för behandlingen, under vilken period som personuppgifterna kommer att lagras, ändamålen med behandlingen, eventuella mottagare som ska ta del av personuppgifterna och den enskildas rätt att inge klagomål till en tillsynsmyndighet.

Alla medarbetare har ett ansvar att tillse att fungerande rutiner kring detta finns.

Upphandling

Vid upphandling och utveckling av IT-tjänster ska kommunen och dess bolag alltid ta hänsyn till dataskyddsförordningen. Detta ska säkerställas i upphandlingsdokument och vid avtalsskrivning. Vid ingång av nya avtal med leverantörer som tillhandahåller program/system där personuppgiftsbehandling ingår ska programmet/systemet upptas i register över behandlingar och personuppgiftsbiträdesavtal upprättas.

Personuppgiftsbiträde

Avtal ska upprättas med de program-/systemleverantörer och eventuellt andra parter som på personuppgiftsansvariges uppdrag hanterar personuppgifter. Part som tecknat avtal med leverantören är ansvarig för att personuppgiftsbiträdesavtal upprättas. Detta innebär att om kommunalförbundet har avtal med en leverantör vars program/system används av samverkande kommuner är det förbundets ansvar att upprätta personuppgiftsbiträdesavtal med leverantören. Om detta förfarande kräver skriftligt avtal i form av fullmakt eller liknande, ska detta upprättas. Kommunalförbundet och kommunerna upprättar egna personuppgiftsbiträdesavtal sinsemellan.

Vid utformning av avtal används företrädesvis den mall för personuppgiftsbiträdesavtal som tagits fram av kommunalförbundet och de samverkande kommunerna. Om leverantören inkommer med förslag till avtal ska det säkerställas att förslaget innehåller motsvarande information som egen avtalsmall.

Den som undertecknar avtalet ska ha adekvat delegering från den personuppgiftsansvarige.

Rapport om personuppgiftsincident

Med personuppgiftsincident avses en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av de personuppgifter som behandlas. Det kan också vara fråga om en personuppgiftsincident om en säkerhetsincident leder till obehörigt röjande av eller obehörig åtkomst till de behandlade personuppgifterna. Det kan exempelvis vara intrång i ett program/system som hanterar personuppgifter eller ett e-postmeddelande med personuppgifter som skickats fel.

Bilaga 1: Riktlinje för behandling av personuppgifter

Alla medarbetare har ett ansvar att rapportera personuppgiftsincidenter enligt gällande rutiner.

När det har inträffat en personuppgiftsincident måste personuppgiftsansvariga först fastställa sannolikheten och allvaret, och den därmed följande risken för människors rättigheter och friheter. Om det är troligt att personuppgiftsincidenten kommer att medföra en risk för de registrerade måste Datainspektionen meddelas inom 72 timmar. Men om det är osannolikt att en personuppgiftsincident medför risker är detta inte nödvändigt. Även om personuppgiftsansvariga inte bestämmer sig för att anmäla incidenten, måste beslutet motiveras och dokumenteras.

Om personuppgiftsincidenten bedöms medföra allvarliga risker för de registrerade ska även de registrerade informeras om händelsen.

Riktlinje antagen tillsammans med *Policy för behandling av personuppgifter* av Kommunfullmäktige 2018-05-28

Reviderad och antagen av Kommunstyrelsen 2018-01-07 Antagen av KF 2019-03-04 § 13