

Policy för behandling av personuppgifter

Antagen av kommunfullmäktige i Surahammars kommun
2018-05-28, § 42

Ansvarig handläggare
Mia Ublin
Utredare
mia.ublin@surahammar.se



Surahammars
kommun



Målsättning för personuppgiftsbehandling

Målet med denna policy är att säkerställa att Surahammars kommun och dess bolag hanterar personuppgifter i enlighet med EU:s dataskyddsförordning (General Data Protection Regulation – GDPR). Policyn omfattar samtliga behandlingar där personuppgifter hanteras och omfattar både strukturerat och ostrukturerat material. Policyn gäller för kommunens nämnder och dess helägda bolag.

Surahammars kommuns mål är att all behandling sker med hänsyn till den enskildes integritet och rättigheter.

Personuppgifter ska behandlas med utgångspunkt i följande principer:

- All behandling ska ske i enlighet med gällande lagstiftning
- Personuppgifter ska endast behandlas för berättigat ändamål som är fastställt innan behandling påbörjas
- Personuppgifter ska vara korrekta och uppdaterade
- Risker för skada för den registrerade ska minimeras genom aktiv riskhantering och lämpliga skyddsåtgärder
- Endast behöriga ska få åtkomst till personuppgifter
- Personuppgifter ska skyddas så de inte oavsiktligen förstörs
- Personuppgifter ska bevaras endast så länge det är nödvändigt för ändamålet
- Inbyggt dataskydd och dataskydd som standard tillämpas genom att ta hänsyn till integritetsfrågor och bygga in lämpliga säkerhetsmekanismer i IT-lösningar
- Överföring till tredje land ska inte ske utan adekvata säkerhetsåtgärder
- Krav på att personuppgifter hanteras enligt gällande lagstiftning ska alltid säkerställas vid upphandling och utveckling av IT-lösningar och tjänster, och ska vara en del i kravspecifikationen och eventuella avtal
- Hantering av personuppgifter ska dokumenteras, följas upp och utvärderas kontinuerligt

Definitioner

Med personuppgift avses information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Exempel på personuppgifter är personnummer, namn, adresser, fastighetsbeteckningar, bild- och ljudupptagningar genom vilka en person kan identifieras. En bedömning om det är fråga om personuppgifter måste göras i det enskilda fallet.

Med behandling av personuppgifter avses åtgärder eller serier av åtgärder som vidtas i fråga om personuppgifter. Exempel på strukturerat material är insamling, registrering, lagring, bearbetning, sammanställning eller samkörning. Även ostrukturerat material, så som personuppgifter som skickas via e-post eller sprids på annat sätt omfattas.

Organisation och ansvar

Kommunstyrelsen beslutar övergripande om viljeinriktningen för personuppgiftsarbetet. Varje styrelse och nämnd är personuppgiftsansvarig för sina egna personuppgiftsbehandlingar. Det vill säga de behandlingar som görs inom styrelsens eller nämndens ansvarsområde. Styrelser och nämnder är ytterst ansvariga för att:

- Följa gällande lagstiftning



Surahammars kommun

- Säkerställa att det finns ett Dataskyddsbud
- Fastställa ändamål med behandlingar
- Säkerställa att behandling sker med lämplig teknisk och organisatorisk säkerhet
- Ansvara för att dokumentation av behandlingar finns (registerförteckning)
- Giltiga personuppgiftsbiträdesavtal finns upprättat vid behov
- Säkerställa att det vid behov görs riskanalyser och konsekvensbedömningar om behandlingar sannolikt medför en hög risk för den registrerades integritet
- Säkerställa att personuppgiftsincidenter rapporteras till tillsynsmyndigheten
- Tillgodose registrerades rättigheter gällande information, tillgång (utlämning), rättning, begränsning, dataportabilitet och invändning
- Tidsfrister sätts och verkställs för behandlingar gällande arkivering, gallring och rensning

Dataskyddsbud

Samtliga personuppgiftsansvariga som enligt lagstiftningen ska utse ett Dataskyddsbud ska göra det. Dataskyddsbud har till uppgift att informera och ge råd till den personuppgiftsansvariga organisationen kring vilka skyldigheter som gäller enligt dataskyddsförordningen. Dataskyddsbudet ansvarar bland annat för kommungemensamma styrdokument och mallar inom området. Dataskyddsbudet ska bevaka att reglerna följs och är kontaktperson för tillsynsmyndigheten. Dataskyddsbudet är en oberoende funktion som ska anmälas till tillsynsmyndigheten.

Dataskyddssamordnare

Dataskyddssamordnare är kommunens kontaktperson gentemot Dataskyddsbudet. Dataskyddssamordnare ska bidra i arbetet med personuppgiftsbehandling utifrån sitt verksamhetsperspektiv, till exempel gällande framtagande av riktlinjer, arbetssätt och övervakning av efterlevnad för personuppgiftsbehandling. Dataskyddssamordnaren ansvarar för att vara insatt i gällande verksamhetsspecifik lagstiftning inom området. Dataskyddssamordnaren ansvarar även för att utbilda, informera och ge råd till verksamheten den representerar.

Samtliga personuppgiftsansvariga ansvarar för att säkerställa att minst en Dataskyddssamordnare är utsedd som kontaktperson inom respektive verksamhetsområde. Dataskyddssamordnare utses av verksamhetschef, verkställande direktör eller motsvarande.

Personuppgiftsbiträde

Personuppgiftsbiträde är program- eller systemleverantör eller annan som på uppdrag av personuppgiftsansvarig hanterar dennes personuppgifter. Med biträdet ska ett personuppgiftsbiträdesavtal upprättas för att säkerställa ändamålsenlig hantering av personuppgifterna.

Vidare anvisningar

Ytterligare information om tillämpning av denna policy återfinns i *Bilaga 1: Riktlinje för behandling av personuppgifter*. Vidare konkretisering av denna policy ska utarbetas i andra riktlinjer för personuppgiftsbehandling.