



Vimmerby
kommun

Policy för hantering av personuppgifter

Antagen av kommunfullmäktige

2022-02-28 § 12

Gäller för: Vimmerby kommunkoncern

Gäller fr o m: 2022-02-28

Version: 0.3

Inledning och syfte

Vimmerby kommuns policy för hantering av personuppgifter gäller för kommunens samtliga nämnder, bolag och stiftelser. Syftet med policyn är att dels säkerställa att kommunen hanterar personuppgifter på ett lagenligt sätt, dels för att visa allmänheten och anställda att de kan känna sig trygga med att deras personuppgifter hanteras på ett säkert sätt.

Vimmerby kommuns policy för hantering av personuppgifter kompletteras av Vimmerby kommuns handbok för hantering av personuppgifter.

Ansvar och organisation

Nämnderna är personuppgiftsansvariga

Varje nämnd, bolag och stiftelse är personuppgiftsansvarig för behandlingen av personuppgifter inom sitt verksamhetsområde. Nämnderna har det yttersta ansvaret för att dataskyddsförordningen efterlevs. Ansvaret innebär bland annat:

- Att innan behandling av personuppgifter påbörjas fastställa ändamål och rättslig grund med behandlingen.
- Att utse dataskyddsombud och svara för att denne har lämpliga förutsättningar och kunskap för att utföra sitt uppdrag.
- Att säkerställa att lämpliga tekniska och organisatoriska säkerhetsåtgärder vidtas för att skydda personuppgifter.
- Att kunna visa efterlevnad av dataskyddsförordningen, bland annat genom att föra register över de personuppgiftsbehandlingar som utförs.
- Att regelbundet genomföra översyn av organisationens efterlevnad av dataskyddsförordningen.
- Att säkerställa att förvaltningen har lämplig organisation, rätt resurser och relevant kompetens inom området för att kunna följa dataskyddsförordningen.

Särskilt om kommunstyrelsen

Kommunstyrelsen har genom sin uppsiktsplikt över nämnderna ett särskilt ansvar för kommunens behandling av personuppgifter. Kommunstyrelsen ska inom ramen för uppsiktsplikten vid behov ge nämnderna råd, anvisningar och förslag på åtgärder.

Kommundirektör

Kommundirektören ansvarar för att den kommunala verksamheten har en fungerande dataskyddsorganisation.

Central dataskyddsamordnare

På kommunledningsförvaltningen (eller motsvarande) ska det finnas en central dataskyddssamordnare med ansvar för att samordna kommunens dataskyddsarbete. Den centrala dataskyddssamordnaren ska ha ett uttalat och dokumenterat uppdrag, samt avsatt arbetstidsmått för att arbeta med dataskyddsfrågor.

Uppdraget innebär att:

- Samordna kommunens dataskyddsarbete (t. ex. gällande riktlinjer, registerförteckning och information till registrerade).
- Hålla kontakt med dataskyddsombudet.
- Delta i Itsams GDPR-nätverk (ca. 4 ggr/år).
- Bistå förvaltningarna med råd och stöd i frågor relaterade till efterlevnaden av dataskyddsförordningen.
- Att identifiera förekomsten av generella svårigheter och problem i förvaltningar och i samråd med dataskyddsombudet ta fram förslag till lämpliga åtgärder.

Lokal dataskyddssamordnare

Varje förvaltning och de kommunala bolagen kan utse minst en lokal dataskyddssamordnare med ansvar för att arbeta löpande med frågor relaterade till dataskyddsförordningen. Lokal dataskyddssamordnare ska ha ett uttalat och dokumenterat uppdrag, samt avsatt arbetstidsmätt för att arbeta med dataskyddsfrågor. Uppdraget innebär att:

- Vara förvaltningens kontaktperson för dataskyddsfrågor.
- Vara länken mellan förvaltningen, den centrala dataskyddssamordnaren och dataskyddsombudet. Exempelvis när en personuppgiftsincident har inträffat.

Dataskyddsombud

Varje nämnd ska utnämna ett dataskyddsombud och anmäla dennes kontaktuppgifter till Integritetsskyddsmyndigheten. X kommun samverkar med Kommunalförbundet Itsam gällande dataskyddsombud, och ska därmed utse denne som dataskyddsombud. Den personuppgiftsansvarige ska säkerställa att dataskyddsombudet i god tid deltar i alla frågor som rör dataskydd, samt tillhandahålls de resurser och det stöd som krävs för att fullgöra sina uppgifter.

Den övergripande och viktigaste uppgiften för dataskyddsombudet är att övervaka att organisationen följer dataskyddsförordningen. Uppdraget innebär bland annat att:

- Samla in information om hur organisationen behandlar personuppgifter.
- Kontrollera att organisationen följer bestämmelser och interna styrdokument.
- I samråd med verksamheterna ta fram styrdokument för dataskydd.
- Informera, utbilda och ge råd inom organisationen.
- Ge råd i riskanalyser och konsekvensbedömningar.
- Ta emot information om misstänkt eller konstaterad personuppgiftsincident och ge råd avseende incidenten under pågående hantering.
- Stödja personuppgiftsansvarig vid upprättandet av personuppgiftsbiträdesavtal.
- Vara kontaktperson för Integritetsskyddsmyndigheten.
- Vara kontaktperson de registrerade och personalen inom organisationen.
- Samarbeta med Integritetsskyddsmyndigheten, till exempel vid tillsyn.
- Sammankalla Itsams GDPR-nätverk (ca. 4 ggr/år)
- Författa och redovisa en årlig rapport om organisationens efterlevnad av dataskyddsförordningen, med förslag på åtgärder.

Dataskyddsbudbet ska kunna arbeta självständigt och oberoende inom organisationen - av den anledningen är det viktigt att dataskyddsbudbet inte har några andra arbetsuppgifter som kan innebära intressekonflikt med rollen som dataskyddsbudbet. Dataskyddsbudbet har inget eget ansvar för att organisationen följer dataskyddsförordningen, det ansvaret ligger alltid hos den personuppgiftsansvariga eller hos personuppgiftsbiträdet. Personuppgiftsansvarig får heller inte bestraffa dataskyddsbudbet för att ha utfört sina arbetsuppgifter.

De grundläggande principerna

I dataskyddsförordningen finns ett antal grundläggande principer som kan sägas vara kärnan i förordningen. Principerna gäller för all personuppgiftsbehandling och sätter de yttersta ramarna för vad som är en tillåten behandling. Personuppgiftsbehandling i kommunen ska alltid genomsyras av följande grundläggande principer:

- Laglighet, korrekthet och öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering
- Riktighet
- Lagringsminimering
- Integritet och konfidentialitet
- Ansvarsskyldighet

Mål för uppföljning

Vimmerby kommuns policy för hantering av personuppgifter kompletteras av Vimmerby kommuns handbok för hantering av personuppgifter. Nedan framgår handbokens mål för uppföljning. Målen ska följas upp årligen.

- Personuppgiftsbehandling ska ske i enlighet med dataskyddsförordningens grundläggande principer.
- Det ska alltid finnas ett ändamål och en rättslig grund för personuppgiftsbehandling.
- Registrerade ska få klar och tydlig information om personuppgiftsbehandlingen.
- Registrerade ska kunna utöva sina rättigheter.
- Vid behandling av barns personuppgifter ska barns särskilda rätt till integritetsskydd beaktas.
- Register över personuppgiftsbehandlingar ska föras och uppdateras kontinuerligt.
- Personuppgiftsincidenter ska uppmärksammas, åtgärdas, dokumenteras – och i vissa fall anmälas.
- Lämpliga tekniska och organisatoriska säkerhetsåtgärder ska vidtas för att skydda personuppgifter, säkerhetsåtgärderna ska reflektera uppgifternas art och risken som behandlingen medför för den registrerade.
- Dataskyddsförordningen ska beaktas innan, under och efter upphandling/inköp av produkter, tjänster, programvaror, applikationer som innebär behandling av personuppgifter.
- Konsekvensbedömning avseende dataskydd ska genomföras om en behandling av personuppgifter sannolikt leder till hög risk för de registrerades fri- och rättigheter.
- När ett personuppgiftsbiträde anlitas ska säkerheten för personuppgifter garanteras och personuppgiftsbiträdesavtal skrivas.