

Januari 2020

Kommunstyrelsen
Gävle kommun

Dataskyddsenheten
Gävle kommun

Dataskyddssombudets årsrapport 2019

Inledning

EU:s dataskyddsförordning 2016/679 (GDPR) började tillämpas den 25 maj 2018 och ersatte genom sitt ikraftträdande Personuppgiftslagen (PUL) (1998:204).

Vid ikraftträdande av dataskyddsförordningen bildades en dataskyddsenhet i Gävle kommun. Vid enheten finns två dataskyddsombud för kommunen samt kommunens bolag och kommunalförbund. Utöver Gävle kommunkoncern och kommunalförbund har dataskyddsombuden även arbetat mot grannkommunerna Hofors och Ockelbo samt deras kommunägda bolag under 2019. Dataskyddsombudens främsta uppgift är att informera och ge råd till personuppgiftsansvariga om deras skyldigheter enligt dataskyddslagstiftningen samt övervaka efterlevnaden av dataskyddslagstiftningen.

Utöver dataskyddsombud ska respektive samverkande organisation ha utsett dataskyddssamordnare som förväntas ha en nyckelroll i det operativa dataskyddsarbetet.

Stödjande arbete

Dataskyddsombudet har under verksamhetsåret gett råd och stöd i löpande frågor som kommit från personuppgiftsansvariga samt genomfört vissa rättsutredningar. Ombudet har även gett råd vid inkommande frågor från allmänheten.

Dataskyddsombudet har genomfört utbildnings- och informationsinsatser riktade antingen mot förtroendevalda, dataskyddssamordnare, ledningsgrupper eller övriga anställda. Generella utbildningar har erbjudits via utbildningskatalogen på Ankaret. Verksamhetsanpassade utbildningar har genomförts efter beställning från verksamheter.

Genomförda generella utbildningar och informationsinsatser:

- Grundläggande dataskyddsutbildning för kommunanställda (3 tillfällen)
- Dataskydd för systemägare (2 tillfällen)
- Dataskydd för chefer och ledningsgrupper (1 tillfälle)
- Dataskydd för kommunikatörer (2 tillfällen)
- Dataskydd för projektledare och verksamhetsutvecklare (2 tillfällen)
- Information till sektorchefer i kommundirektörens ledningsgrupp (1 tillfälle)

Genomförda verksamhetsspecifika informationsinsatser

- Information till IT-avdelningen
- Information till kommunarkivet och kanslienheten
- Information till Kommunstyrelsen vid nämndsammanträde

Övriga verksamhetsspecifika insatser

Dataskyddsombudet har gett Kommunstyrelsen råd avseende bl.a. fördelning av personuppgiftsansvar i systemet Platina, personuppgiftsbiträdesavtal, IT-avdelningens roll i dataskyddsarbetet, säkerhetsåtgärder vid hantering av känsliga uppgifter i verksamhetssystem, publicering av personuppgifter på webben, dataskydd i arbetet med stiftelsefonder samt inhämtande av samtycke vid personuppgiftsbehandling i olika sammanhang.

Konsekvensbedömningar

Om en behandling av personuppgifter sannolikt leder till hög risk för de registrerades fri- och rättigheter måste personuppgiftsansvariga göra en konsekvensbedömning enligt dataskyddsförordningen. En konsekvensbedömning är en dokumenterad risk-och sårbarhetsanalys utifrån ett dataskyddsperspektiv. Dataskyddsombudets uppgift under en konsekvensbedömning är att ge råd samt övervaka att konsekvensbedömningens innehåll uppfyller kraven i dataskyddsförordningen. Personuppgiftsansvariga är skyldiga att samråda med dataskyddsombudet i samband med en konsekvensbedömning. Dataskyddsombudet har utformat stöddokument för konsekvensbedömningar.

Kommunstyrelsen har under 2019 enligt dataskyddsombudets kännedom påbörjat konsekvensbedömningar avseende verksamhetssystemet Adato samt Masterdata (i egenskap av personuppgiftsbiträde). Dataskyddsombudet har gett rekommendationer avseende säkerhetsåtgärder i Adato.

Dataskyddsbudet rekommenderar Kommunstyrelsen att inventera vilka pågående eller planerade personuppgiftsbehandlingar nämnden har som kan innebära hög risk för registrerades fri- och rättigheter och genomföra konsekvensbedömningar för sådana behandlingar.

Personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks exempelvis genom diskriminering, identitetsstöld, bedrägeri, skadlig ryktesspridning, finansiell förlust, brott mot sekretess eller tystnadsplikt. En personuppgiftsincident har till exempel inträffat om personuppgifter har, blivit förstörda, gått förlorade på annat sätt eller röjts till någon obehörig.

Vissa personuppgiftsincidenter måste anmälas till Datainspektionen, och anmälan måste ske inom 72 timmar från det att överträdelsen upptäckts. En personuppgiftsincident behöver inte anmälas till Datainspektionen om det är osannolikt att incidenten medför en risk för fysiska personers fri- och rättigheter.

Dataskyddsbudet har gett råd i samband med personuppgiftsincidenter i de fall personuppgiftsansvariga har samrått med ombudet. Kommunstyrelsen har under 2019 samrått med dataskyddsbudet avseende nio personuppgiftsincidenter varav nämnden beslutat att anmäla sex incidenter till Datainspektionen.

Övervakande arbete

Dataskyddsbudet har genomfört följande granskningar hos Kommunstyrelsen i enlighet med granskningsplanen för 2019:

- Registerförteckning
- Dataskyddsorganisation

Granskningarna har sammanfattats och redovisats genom skriftliga rapporter. Rapporterna har skickats för kännedom till Kommunstyrelsen. I de fall dataskyddsbudet har identifierat brister eller utvecklingsområden i den personuppgiftsansvariges personuppgiftshantering har rekommendationer om förbättringsåtgärder lämnats i rapporterna.

Dataskyddsbudet har därutöver i september 2019 påbörjat en granskning av Kommunstyrelsens efterlevnad av informationskyldigheten. Kommunstyrelsen har önskat anstånd med att besvara frågorna till slutet av januari 2020 och granskningen har därmed ännu inte kunnat fullföljas av dataskyddsbudet.

Omvärldsbevakning

Dataskyddsbudet har under verksamhetsåret deltagit i nätverksträffar där dataskyddsbud från ett antal olika myndigheter i regionen deltagit. Dataskyddsbudet har bevakat praxis och nyheter och informerat de personuppgiftsansvariga organisationerna när informationen varit relevant för dem.



Utveckling av arbetet

Rapportering direkt till personuppgiftsansvariga

Dataskyddsombudet ska enligt art. 38 i dataskyddsförordningen rapportera direkt till den personuppgiftsansvariges högsta förvaltningsnivå, vilket hos kommunala organisationer betyder nämnd/styrelse. Dataskyddsombudet har hittills använt sig av följande metoder för rapportering; årsrapport, granskningsrapport samt information på ett nämnd- eller styrelsesammanträde om nämnden/styrelsen så önskat. Rapporteringssätt och regelbundenheten kan utökas och utvecklas om den personuppgiftsansvarige så önskar.

I tjänsten

Parisa Maleki Nordin
Dataskyddsombud
Gävle kommuns dataskyddsenhet