2020-12-07

Socialnämnden, Omvårdnadsnämnden och Arbetsmarknads- och funktionsrättsnämnden i Gävle kommun

Granskning av dataskyddsorganisation

Dataskyddsenheten har genomfört en uppföljning av tidigare granskningar och granskning av personuppgiftsansvarigas systematiska arbete med personuppgiftsincidenter, som en del av dataskyddsenhetens övervakande arbete 2020. Granskningen har genomförts hos flertalet personuppgiftsansvariga organisationer inom dataskyddsenhetens arbetsområde.

Under 2019 granskade Dataskyddsenheten personuppgiftsansvarigas register över personuppgiftsbehandlingar och dataskyddsorganisation. Dataskyddsenheten har under 2020 genomfört en uppföljning om personuppgiftsansvariga har genomfört nödvändiga åtgärder i enlighet med tidigare rekommendationer från Dataskyddsenheten.

Sektor Välfärd har granskats genom intervju av dataskyddssamordnare och chef vid Administrativt stöd.

Uppföljning av dataskyddsorganisation

Enligt artikel 24 i dataskyddsförordningen följer att den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att organisationens personuppgiftsbehandlingar följer dataskyddsförordningen.

Enligt artikel 5.2 ska den personuppgiftsansvarige kunna visa att all personuppgiftsbehandling följer de viktiga grundprinciperna för personuppgiftsbehandling (laglighet och öppenhet, ändamålsbegränsning, uppgiftsminimering, korrekthet, lagringsminimering samt integritet och konfidentialitet enligt art. 5)

Dataskyddsombudets bedömning:

De förtroendevalda i kommunala nämnder är personuppgiftsansvariga enligt dataskyddsförordningen. Den högsta ledningen under respektive nämnd ansvarar normalt för verkställigheten av de arbetsuppgifter som följer av personuppgiftsansvaret och har därmed en nyckelroll i organisationens dataskyddsarbete. Det är av vikt att högsta ledningen tar en aktiv roll i dataskyddsarbetet

genom att ta initiativ till regelbunden återkoppling från dataskyddssamordnare om framtida och genomförda aktiviteter.

Vid tidigare granskning genomgick personuppgiftsansvariga en omorganisation vilket ledde till att en dataskyddsorganisation inte hade implementerats inom hela sektorn. Det saknades utsedd dataskyddssamordnare för Omvårdnadsnämnden och Arbetsmarknads- och funktionsrättsnämnden. Nu har tidigare dataskyddssamordnare för Socialnämnden tagit över ansvaret som dataskyddssamordnare för alla nämnder inom sektorn. Utöver har tre medarbetare vid dataskyddssamordnares enhet fått i uppdrag att stötta med det löpande dataskyddsarbetet, så som registerutdrag, incidenter, etc. Sektorn är uppdelad i fem kontor där det finns utsedda dataskyddskoordinator vid varje kontor.

Sektor Välfärd har utrett frågan om roller och ansvar enligt de rekommendationer som lämnades vid tidigare granskning.[1] Det är positivt att roller och ansvar är tydligt dokumenterade för att säkerställa att alla personer som är delaktig i dataskyddsarbetet har en klar rollfördelning sinsemellan men även tid och kompetens för arbetet. Det är tveksamt om dataskyddssamordnare har tillräckligt med tid utöver tidigare ordinarie arbetsuppgifter. Om kompetens koncentreras till en person blir organisationen även sårbar samt riskerar man att dataskyddsarbete inte fortlöper i önskvärd takt. Om exempelvis enbart en medarbetare vid hela sektorn har kompetens för att leda en konsekvensbedömning och personen är otillgänglig på grund av otillräckligt med tidsutrymme eller annan orsak kan inte en behandling påbörjas utan att riskera bristande dataskydd.

I dokumentation över dataskyddsorganisationens roller har dataskyddssamordnare rollen att driva dataskyddsfrågor inom verksamheten, uppdatera register och sköta helhetssynen på vad som sker inom förvaltningen.[2] Sektorn är en stor och komplex organisation, det kan riskera att bli en flaskhals om en person ska initiera och leda allt dataskyddsarbete.

Ledning bör genomföra en översyn av dataskyddsorganisationen för att säkerställa att varje person har tid för dataskyddsarbetet. Exempel på åtgärder som ledningen kan ta för att säkerställa ett dataskyddsarbete som fortskrider i önskvärd takt är att:

(1) Överföra ansvar ner i organisationen.
(2) Utse fler dataskyddssamordnare.
(3) Frigöra tid för dataskyddssamordnare.

[1] *Slutrapport för Roller GDPR, 2019-06-12*
[2] Bilaga 1, Rollbeskrivningar* samt organisationsförslag A och B

Att en nyckelpersonen för dataskyddsarbete, dataskyddsamordnaren i det här fallet, inte har tillräckligt med tid för sitt uppdrag kan riskera sektorns framgång i dataskyddsarbetet. Ledningen kan genomföra andra åtgärder än den ovanstående förslagen utifrån organisationens behov och möjligheter men bedömningen är att tidsutrymme måste skapas.

Dataskyddsombudets rekommendation:

Ledning bör utvärdera den redan implementerade dataskyddsorganisation.

Uppföljning av registerförteckning

Enligt artikel 30 i dataskyddsförordningen ska personuppgiftsansvariga föra ett register över personuppgiftsbehandlingar som utförs under dess ansvar.

Dataskyddsombudets bedömning:

Vid tidigare granskning bedömdes Socialnämnden ha en inkomplett registerförteckningen då den saknade den grundläggande informationen som en registerförteckning ska ha i enlighet med artikel 30. Omvårdnadsnämnden och Arbetsmarknads- och funktionsrättsnämnden saknade registerförteckningar.

Socialnämnden har efter tidigare granskning kompletterat registerförteckningen med den grundläggande informationen i ett exceldokument. För kartläggning av personuppgiftsbehandlingar utgick Socialnämnden från verksamhetsprocesser och dokument där personuppgifter framgick. En processbaserad dokumentation kan användas för att skapa en tydligare bild över de faktiska behandlingar man har för att inte av misstag genomföra flera behandlingar med olika rättsliga grunder i ett system. Alternativt att en personuppgiftsbehandling är dokumenterad som flera personuppgiftsbehandlingar i registerförteckningen men med olika lagringsplatser. Det är däremot viktigt att man inte helt likställer verksamhetsprocesser med personuppgiftsbehandlingar utan tar hänsyn till att man kan dela upp en process inom verksamheten med flera personuppgiftsbehandlingar.

Omvårdnadsnämnden och Arbetsmarknads- och funktionsrättsnämnden saknar fortfarande en komplett registerförteckning. För tillfället pågår ett arbete med att upprätta personuppgiftsbehandlingar för alla tre nämnder i systemet DraftIT som även flertalet andra personuppgiftsansvariga inom Gävle kommunkoncern använder sig av. Det är positivt att man nu ser över alla tre nämnders registerförteckningar och använder ett system som kan öka regelefterlevnaden av Dataskyddsförordningen.

Dataskyddsombudets rekommendation:

Engagerar hela verksamheten för att registerförteckningen ska vara aktuell och komplett.

Fortsatt arbeta processbaserat med förteckningen.

Granskning av personuppgiftsansvarigas systematiska arbete med personuppgiftsincidenter.

Enligt artikel 33.1 i dataskyddsförordningen ska den personuppgiftsansvarige vid en personuppgiftsincident utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig i enlighet med artikel 55, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen.

Enligt artikel 34.1 om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten.

Dataskyddsombudets bedömning

Personuppgiftsansvarig har en upprättad rutin i verksamhetssystemet Canea. Vid en personuppgiftsincident kontaktas dataskyddssamordnare som leder processen. Efter samråd med dataskyddsombud beslutas det om incidenten ska rapporteras till Datainspektionen och om registrerade ska informeras. Efter dokumentation informeras ledning om incidenten. Sammanfattningsvis bedöms sektorn ha en välfungerande process för att anmäla personuppgiftsincidenter.

Problem som kan uppstå i processen är att utredning av incident kan dra ut på tiden och i vissa fall missa tidsramen för att anmäla till Datainspektionen från att man fått vetskap om incidenten.

En systematisk uppföljning av relevanta personuppgiftsincidenter har inte skett. En relevant personuppgiftsincident kan betraktas som en incident där det innebär en risk för de registrerades fri- och rättigheter samt där sannolikheten för att incidenten ska uppstå igen är högre på grund av incidentens art. Vid incident bör dokumentering göras om uppföljning över exempelvis rutiner som implementerats i samband med incident eller att en incident som sker frekvent ska ses över.

Mörkertalet av dokumenterade personuppgiftsincidenter bedöms som lågt inom Socialnämndens verksamheter. Inom Omvårdnadsnämnden och Arbetsmarknads- och funktionsrättsnämnden bedöms mörkertalet vara högre. Bedömningen görs utifrån verksamhetens art och storlek. Att en verksamhet har ett lågt antal dokumenterade personuppgiftsincidenter tyder inte på att man inte begår misstag utan att man misslyckas med att belysa dem. Det beror troligtvis på en bristande dataskyddskultur och för att motverka detta bör personal utbildas inom området för att öka medvetandegraden bland anställda.

Dataskyddsombudets rekommendationer:

Att genomföra kunskapshöjande insatser för anställda med målet att öka kännedom om dataskydd bland anställda.

Att rutin för en systematisk uppföljning av relevanta personuppgiftsincidenter införs.

I tjänsten,

Adrian Vinsa
Dataskyddsombud
Gävle kommuns dataskyddsenhet