



Tjänsteskrivelse

2021-06-08

Diarienummer: 21ON185

Handläggare:

Dunia Fällgren Lopez
026-17 94 86
dunia.fallgren_lopez@gavle.se

Nämnd:

Omvårdnadsnämnd

Åtgärder efter granskning av dataskyddsorganisation

Sammanfattning av ärendet

Dataskyddsenheten på Styrning och Stöd genomförde en uppföljning av tidigare granskningar och granskning av personuppgiftsansvarigas systematiska arbete med personuppgiftsincidenter, som en del av dataskyddsenhetens övervakande arbete 2020.

Rapport av granskning av dataskyddsorganisation inom Omvårdnadsnämnden, diarienummer 20ON413, presenterades för nämnden som ett anmälningsärende den 2020-12-17.

Här följer återkoppling på åtgärder som vidtagits efter nämnd granskning.

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.

Sammanfattning av 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 data-skyddssamordnare om framtida och genomförda aktiviteter.

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.

Dataskyddsombudets rekommendation

Ledning bör utvärdera den redan implementerade dataskyddsorganisationen.

Åtgärd från verksamheten

Kompensöverföring sker mellan medarbetare inom enhet för informationshantering för att säkerställa att alla inom enheten kan handlägga personuppgiftsincidenter samt begäran om registerutdrag. Rekrytering pågår sedan 2021-04-16 av samordnare för informationssäkerhet och dataskydd.

Inom sektor Vårldataskyddsorganisation finns det, förutom dataskyddssamordnare, även dataskyddskoordinatorer. Beroende på kontor finns de på verksamhetsnivå eller enhetsnivå. Arbete med att utbilda dataskyddskoordinatorer är ett prioriterat arbete under kommande höst.

Uppföljning av registerförteckning

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

Sammanfattning av dataskyddsombudets bedömning

Vid tidigare granskning (2019) bedömdes Omvårdnadsnämnden sakna registerförteckning.

Omvårdnadsnämnden saknar fortfarande en komplett registerförteckning (2020). För tillfället pågår ett arbete med att upprätta registerförteckning över personuppgiftsbehandlingar för nämnden i systemet DraftIT som även flertalet andra personuppgiftsansvariga inom Gävle kommunkoncern använder sig av. Det är positivt att man nu ser över nämndens registerförteckning och använder ett system som kan öka regelefterlevnaden av Dataskyddsförordningen.

Dataskyddsombudets rekommendation

Engagera hela verksamheten för att registerförteckningen ska vara aktuell och komplett. Fortsätt arbeta processbaserat med förteckningen.

Åtgärd från verksamheten

Arbete med att slutföra den processbaserade registerförteckningen i DraftIT pågår. Ansvaret för förvaltning av registerförteckning kommer fortsatt att vara hos enheten för informationshantering.

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.

Sammanfattning av dataskyddsombudets bedömning

Personuppgiftsansvarig har en upprättad rutin i verksamhetssystemet Canea One. 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 Datainspektionen¹ från att man fått vetskap om incidenten. En systematisk uppföljning av relevanta personuppgiftsincidenter har inte skett. 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.

Inom Omvårdnadsnämnden bedöms mörkertalet av dokumenterade personuppgiftsincidenter vara högre jämfört med Socialnämndens som bedöms som låga.

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.

Åtgärd från verksamheten

En digital GDPR-utbildning där även informationssäkerhet ingår finns tillgänglig för alla medarbetare i Kompetensen. Information om detta har publicerats på intranätet.

Det finns även uppdaterad information, om vad som gäller kring dataskydd och hur medarbetare praktiskt ska hantera personuppgifter, på Valfärd Gävles GDPR-sidor på intranätet.

Att anmäla en personuppgiftsincident har blivit enklare i och med att anmälningsformulär har skapats och publicerats på ovan nämnda sida.

¹ Datainspektion bytte namn till Integritetsskyddsmyndigheten per 2021-01-01.

Team (i Microsoft Teams) Dataskyddskoordinator-Välfärd Gävle, skapades 2019-12-09 för utsedda dataskyddskoordinatorer, dvs kontaktpersoner för kollegor vid frågor rörande GDPR, och främst vid incidenter eller misstänkta incidenter. Här publiceras också information som rör dataskydd.

Utbildningsinsatser sker, på initiativ av enheter, av dataskyddssamordnare och har under året genomförts dels på plats, dels digitalt via Teams, beroende på aktuella restriktioner (pandemi).

För att mäta om (ökad) kännedom finns om dataskydd bör enheten för informationshantering framöver ta hjälp av verksamhetsutvecklare för att t.ex. skapa en enkät till alla anställda. Utifrån resultat kan ytterligare insatser förutom digital GDPR-utbildning, information på Ankaret samt anpassade enhetsutbildningar planeras och genomföras.

Frågan har även ställts till HR via dataskyddsombud om det är möjligt att introduktion om GDPR och informationssäkerhet kan komma med i olika checklistor för nyanställda inom kommunen.

Vad gäller rutin för en systematisk uppföljning av relevanta personuppgiftsincidenter görs åtgärder i de flesta fall i samband med incidenten varför detta arbete inte har prioriterats. Dock kommer ansvaret med att skapa en rutin läggas på den framtida samordnaren för informationssäkerhet och dataskydd. Föreslagna åtgärder är enkät till alla anställda, analysrapporter samt ta hjälp av verksamhetsutvecklare i detta arbete.

Slutligen planeras ett arbete framöver med att skapa en gemensam process för alla typer av incidenter/ avvikelser/ oönskade händelser där upplägget på uppdraget är att i steg 1, undersöka hur kompetensen ser ut bland chefer och medarbetare gällande incidenter/ avvikelser/ oönskade händelser – ta reda på i vilken mån man har förståelse.

I Steg 2, planerar man testa hur ett urval av incidenter/ avvikelser/ oönskade händelser kan hanteras på ett hållbart sätt inom olika verksamheter - så att vi rapporterar av rätt anledning, inte för sakens skull.

Följande delar planeras levereras i arbetet:

- Definitioner av de olika begreppen - incidenter/ avvikelser/ oönskade händelser
- Beskrivning av hur olika incidenter/ avvikelser/ oönskade händelser förhåller sig till varandra
- Förslag på olika enkla lösningar att hantera incidenter/ avvikelser/ oönskade händelser för chefer och medarbetare.
- Flera deltester av olika typer av incidenter/avvikelser/oönskade händelser och hur dessa skall utvärderas och bli en del i det systematiska kvalitetsarbetet.

Catrin Krsticevic Tranberg

Verksamhetschef

Utveckling och stöd

Sektor Velfärd