2021-12-16

Socialnämnden, Omvårdnadsnämnden och Arbetsmarknads- och funktionsrättsnämnden i Gävle kommun

Granskning av dataskyddsarbete 2021

Dataskyddsombudet har 2021 genomfört en granskning av Sektor Välfärds dataskyddsarbete. En uppföljning av två års tidigare granskningar under 2020 respektive 2019 har även genomförts.

Sektor Välfärd har granskats genom intervju av dataskyddssamordnare.

Granskningen 2021 har fokuserat på två olika huvudområden: personuppgiftsansvarigas information om personuppgiftsbehandlingar till de anställda samt genomförda konsekvensbedömningar. Detta har skett som en del av dataskyddsombudets övervakande arbete 2021. Granskningen har genomförts hos flertalet personuppgiftsansvariga organisationer inom dataskyddsenhetens arbetsområde.

Det övervakande arbetet under 2020 involverade granskning av personuppgiftsansvarigas systematiska arbete med personuppgiftsincidenter och personuppgiftsansvarigs dokumentation av personuppgiftsbehandlingar, s.k. registegisterförteckning. Dataskyddsombudet har under 2021 genomfört en uppföljning om personuppgiftsansvariga har genomfört nödvändiga åtgärder i enlighet med tidigare rekommendationer från dataskyddsombudet.

Uppföljning av registerförteckning

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

Dataskyddsombudets bedömning

Vid granskningen 2020 saknade Arbetsmarknad- och funktionsrättsnämnden (AFN) samt Omvårdnadsnämnden (ON) en registerförteckning. Socialnämnden (SN) hade kompletterat registerförteckning enligt de rekommendationer dataskyddsombud lämnat 2019 om att komplettera registerförteckningen för att uppfylla de krav på registerförteckning som fastställs i artikel 30.

Vid granskning 2021 har alla tre nämnder en registerförteckning som uppfyller de krav som fastställs i artikel 30. Dokumentationen har förts över från Excel till systemet DraftIT Records för bättre dokumentationsmöjligheter, säkerhet samt likt övriga inom kommunkoncernen. Socialnämnden har även övergått från att dokumentera behandlingar där de likställs med system och

lagringsytor för att i stället dokumentera utifrån verksamhetsprocesser i enlighet med rekommendationen från 2020.

En registerförteckning är det mest grundläggande verktyget organisationer kan använda sig av för att säkerställa regelefterlevnad av dataskyddsförordningen samt uppfylla ansvarsprincipen, artikel 5.2, den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna i dataskyddsförordningen följs.

För att en registerförteckning ska kunna användas av organisationen för att uppfylla övriga krav i förordningen bör ansvaret för dokumentation av behandlingar fördelas ut till verksamhetskunniga inom behandlingarna (verksamhetsprocesserna) då i dagsläget är tidigare dataskyddssamordnare satt som ansvarig för alla behandlingarna. En sådan åtgärd kan förhindra att dokumentationen i ett längre perspektiv förlorar aktualitet, förutsatt att man inför rutin om kontinuerlig översyn av behandlingarna. Förslagsvis en gång per år, där ansvarig ser över dokumentationen och uppdaterar inaktuell information. En sådan rutin är även lättare att i nuläget implementera i och med övergången till det nya systemet tillskillnad från tidigare år där excelfiler användes för dokumentation.

Dataskyddsombudets rekommendation

Inför en rutin för kontinuerlig översyn av registerförteckningen.

Uppföljning 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

Sektor Välfärd har en välfungerande process för att dokumentera och anmäla personuppgiftsincidenter. Vid granskning 2020 bedömdes det att vid utredning kan organisationen missa tidsramen för att anmäla till tillsynsmyndigheten inom 72 timmar från att man fått vetskap om personuppgiftsincidenter. Under 2021 har processen förbättrats då allt från att personuppgiftsincidentenen upptäckts, utredningen genomförts och eventuell anmälan, har skett inom tidsramen i högre utsträckning från tidigare år.

För att upptäcka incidenter inom verksamheten, är det av vikt att medarbetare vet vad personuppgifter är, vad personuppgiftsincidenter är och hur man

anmäler dem. Detta för att säkerställa att alla personuppgiftsincidenter inom verksamheten upptäcks. I dagsläget finns möjlighet för medarbetare att ta del av e-utbildning inom dataskydd via Gävle kommuns plattform, Kompetensen på intranätet.

För närvarande finns ett utkast till projektplan avseende möjligheterna till en helöversyn av verksamhetsavvikelser inom sektorn där personuppgiftsincidenter är ett perspektiv vilket är positivt. Avvikelser inom en verksamhet kan primärt fokusera på en typ av avvikelse men kan ursprungligen eller delvis bero på bristande information, att information inte varit tillgänglig, förlorats eller ändrats. Detta gör att en typ av verksamhetsavvikelse även kan vara en personuppgiftsuppgiftsincident.

Dataskyddsombudets rekommendation

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

Personuppgiftsansvarigas information om personuppgiftsbehandlingar till anställda

Enligt artikel 13 och 14 ska personuppgiftsansvarig informera registrerade om vilka personuppgifter organisationen behandlar om dem. Artikel 13 berör när information inhämtas direkt från den registrerade och artikel 14 när information inhämtas från någon annan än den registrerade.

Arbetsgivare behandlar anställdas personuppgifter för att fullfölja åtaganden utifrån arbetsrätten samt andra lagar och regler som styr verksamheten. Granskningen syfte är att säkerställa att arbetsgivaren är tydlig och transparent över hur de informerar personal om arbetsgivarens personuppgiftsbehandling.

Dataskyddsombudets bedömning

Personaladministration
Vid anställning lämnar personuppgiftsansvarig information om personuppgiftsbehandling som framgår av anställningsavtal, där genom anställning och arbete kommer den registrerades uppgifter behandlas i olika verksamhetssystem och kan delas med personuppgiftsbiträden. Syftet/ändamålet är att uppfylla anställningsavtal, kollektivavtal, arbete med verksamhetsutveckling och statistik samt att man kommer behandla uppgifterna tillsvidare.

För tydligare information om personuppgiftsbehandling hänvisas man till tre olika källor, två dokument på intranätet och till den kommunala hemsidan om dataskydd. Personuppgiftsansvariga bör revidera informationen till anställda rörande den generella personaladministrationen så att en komplett information ges till en anställd utifrån dennes perspektiv, förslagsvis enbart på intranätet.

Utöver informeras den registrerade via anställningsavtalet att uppgifter om IT-aktiviteter registreras för kontroll och analys vid fel och för dimensionering av nät. Även kontaktuppgifter om den registrerade kan komma att publiceras på kommunens webbplats.

Att informeras via en två-lager process utifall informationen om dataskydd skulle ta över dokumentet är fullt acceptabelt om information som den registrerade når via länk är relevant för den anställde och inte generell information till allmänheten. Vad personuppgiftsansvariga bör beakta är huruvida alla medarbetare ser information på intranätet som ett naturligt sätt att tillskansa sig information. Frågan frångår den faktiska möjligheten för dem att få tillgång till informationen utan hur lättillgänglig information är utifrån skäl 39 i dataskyddsförordningen mening. Det kan då möjligtvis leda till att arbetsgivaren inte uppfyller kravet om transparens gentemot de registrerade enligt artikel 12.1.

Passagesystem

Personuppgiftsansvarig använder passagesystem, där syftet är att förhindra obehöriga från att få tillgång till lokaler. En personuppgiftsansvarig kan ha flera syften för ett passagesystem, exempelvis besöksstatistik för dimensionering av anläggningar, serviceutbud eller kontroll av vilka som befunnit sig i lokalen i samband med brott, brand eller annan händelse.

När en anställd hämtar en tagg/nyckel för att få tillgång till personuppgiftsansvarigs lokaler får personen ett kvitto där det framgår vilka regler som gäller vid användning. Informationen om personuppgiftsbehandlingen framgår inte på kvittot den anställde erhåller. Tidigare lösning om 2-lager information rekommenderas där den väsentliga informationen framgår. Europeiska dataskyddsstyrelsen rekommenderar att personuppgiftsansvarigs identitet, ändamål med behandling och den registrerades rättigheter framgår i det första lagret. Även annan information som kan överraska den registrerade, så som exempelvis mottagare bör framgå. Det är av vikt att ändamål med behandlingen framgår, inte enbart för vad man ämnar göra med personuppgifterna men det informerar implicit vad man inte ämnar göra.

Övervakning av anställdas datorer och e-post

En arbetsgivare har rätt att följa upp att regler och rutiner följs. Det betyder att arbetsgivaren kan få kontrollera en anställds dator. En individs rätt till privatliv regleras i Europakonventionen, artikel 8 vilket fastställer att en anställd har rätt till skydd för sin kommunikation och sitt privatliv. Enbart vid allvarlig misstanke om illojalt eller brottsligt beteende kan det vara tillåtet att ta del av själva innehållet i de anställdas privata filer eller e-postmeddelanden. För att en arbetsgivare ska få kontrollera anställdas datorer måste den anställda ha fått tydlig information i förväg om vilka kontroller som kan komma att ske, till exempel om man kan komma ta del även av innehållet i filer eller e-post. En arbetsgivare bör generellt lägga större fokus på förebyggande åtgärder än på att upptäcka missbruk i efterhand.

Personuppgiftsansvarig lämnar i samband med anställningsavtal information om att IT-aktiviteter kontrolleras men ändamålet är för att analysera fel och dimensionering av nät vilket den genomsnittlige anställde troligt inte uppfattar som läsning av filer och e-post. Rutin för hur anställda använder sig av arbetsgivarens verktyg kan vara ett lämpligt sammanhang att informera om möjligheten till kontroll.

Övervakning i IT-system

I *Rutin för loggkontroll* för system som Treserva och NPÖ, framgår det att kunskap hos medarbetare om förekomsten av loggkontroller är en förebyggande åtgärd under förutsättningen att användarna informeras. Det kan inom yrkesutövningen förväntas att denna kunskap finns men det bör kompletteras med hur det faktiskt sker i realiteten. Det kan minska risken att det finns en skillnad mellan rutin och hur den faktiska verksamheten fungerar.

Dataskyddsombudets rekommendation

Komplettera information om personuppgiftsbehandling vid personaladministration till anställda.

Genomför översyn över hur anställda informeras om personuppgiftsbehandlingen i passagesystem.

Fastställ rutin över hur anställda får använda sig av arbetsgivarens datorer och e-post samt informera anställda om rutin.

Komplettera rutin för loggkontroll med att klargöra hur information lämnas till användare.

Konsekvensbedömningar avseende dataskydd

Enligt artikel 35 i Dataskyddsförordningen, om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En enda bedömning kan omfatta en serie liknande personuppgiftsbehandlingar som medför liknande höga risker.

Den personuppgiftsansvarige ska rådfråga det utsedda dataskyddsombudet, vid genomförande av en konsekvensbedömning.

Dataskyddsombudet har granskat om personuppgiftsansvarig har genomfört konsekvensbedömningar på de personuppgiftsbehandlingar som sannolikt leder till en hög risk. Dataskyddsombudet har utgått ifrån Integritetsskyddsmyndighetens förteckning av kriterier över när en konsekvensbedömning ska genomföras.

En konsekvensbedömning är ett verktyg som ger personuppgiftsansvarig möjlighet att uppfylla de grundläggande principerna om dataskydd i artikel 5.1 samt även principen om ansvarsskyldighet i artikel 5.2, alltså att man kan visa och bevisa att man följer lagstiftningen.

Dataskyddsombudets bedömning

Personuppgiftsansvariga har genomfört ett flertal konsekvensbedömningar enligt artikel 35. Dataskyddsorganisationen fokuserar på att genomföra konsekvensbedömningar på behandlingar som kommer att implementeras i samband med upphandling av nya system. De personuppgiftsbehandlingar där personuppgiftsansvarig inte genomfört en konsekvensbedömning men

uppfyller mer än två kriterier är behandlingar i systemen Treserva och Tieto som alla nämnder har behandlingar i samt AFN som använder Canvas. Konsekvensbedömning för behandlingar i Treserva har delvis genomförts men inte alla behandlingar i systemet. Det är en prioriteringsfråga över vilka konsekvensbedömningar som kommer genomföras och att fokus ligger på nya behandlingar är rimligt men de behandlingar som finns i ovanstående system är omfattande i relation till verksamheten och bör genomföras för att säkerställa att man beaktat alla risker som behandlingarna medför.

Kriterierna som anses uppfyllda är något av följande, omfattande i relation till verksamheten, behandlar känsliga personuppgifter enligt artikel 9, människor i en utsatt position eller i en beroendeställning. Samt använder ny teknik eller nya organisatoriska lösningar.

Personuppgiftsansvarig bör även i sin registerförteckning över personuppgiftsbehandlingar dokumentera alla personuppgiftsbehandlingar utifrån om de uppfyller kriterierna eller inte för när en konsekvensbedömning ska genomföras. Detta för att säkerställa att man genomfört konsekvensbedömning på alla behandlingar och medföljande risker. Om de uppfyller minst två men väljer att inte genomföra en, ska de motivera samt inhämta dataskyddsombudets synpunkter.

Rekommendation

Komplettera registerförteckning utifrån vilka personuppgiftsbehandlingar som uppfyller kraven för när konsekvensbedömning ska genomföras.

Genomför konsekvensbedömning på de personuppgiftsbehandlingar som uppfyller kraven när en konsekvensbedömning ska genomföras i de identifierade verksamhetssystemen.

I tjänsten,

Adrian Vinsa
Dataskyddsombud
Gävle kommuns dataskyddsenhet