2022-06-09

Socialnämnden, Omvårdnadsnämnden och Arbetsmarknads- och funktionsrättsnämnden i Gävle kommun

Granskning av dataskyddsarbete 2022

Dataskyddsombudet har 2022 genomfört en granskning av Sektor Välfärds dataskyddsarbete. En uppföljning av två års tidigare granskningar under 2021 respektive 2020 har även genomförts.

Sektor Välfärd har granskats genom intervju av dataskyddssamordnare.

Granskningen 2022 har fokuserat på två olika huvudområden: uppföljning av personuppgiftsbiträden och dess personuppgiftsbiträdesavtal samt rättsliga grunder. Detta har skett som en del av dataskyddsombudets övervakande arbete 2021. Granskningen har genomförts på liknande sätt hos flertalet personuppgiftsansvariga organisationer inom dataskyddsenhetens arbetsområde.

Under 2020 granskade dataskyddsombudet personuppgiftsansvarigs systematiska arbete med personuppgiftsincidenter. Under 2021 granskades den information om personuppgiftsbehandlingar personuppgiftsansvarig i rollen som arbetsgivare lämnar till anställda samt konsekvensbedömningar avseende dataskydd.

Granskningens syfte är att kontrollera hur personuppgiftsansvariga arbetar strategiskt med dataskyddsfrågor samt hur det systematiska arbetet med dataskydd är organiserat hos personuppgiftsansvariga.

Granskning av personuppgiftsansvariges uppföljning av personuppgiftsbiträden och dess personuppgiftsbiträdesavtal

Ett så kallat personuppgiftsbiträdesavtal, ”PUB-avtal”, är ett avtal som den personuppgiftsansvarige, dvs respektive nämnd, kommunalt bolag och kommunalförbund, enligt GDPR artikel 28 måste upprätta med samtliga personuppgiftsbiträden, exempelvis externa leverantörer av IT-tjänster som behandlar den personuppgiftsansvariges personuppgifter. Avtalen, som inte får vara muntligt, reglerar hur biträdet får behandla personuppgifterna och vilka extra skyddsåtgärder som behöver vidtas. Avtalet reglerar även om personuppgifter får överföras till tredjeland. Dataskyddsombudet rekommenderar att använda de mallar som Sveriges kommuner och regioner, SKR, tillhandahåller. Detta då de är korrekta och balanserade mellan parterna.

Personuppgiftsansvarig har efter upphandling av tjänst och tecknande av biträdesavtal fortfarande ansvar för att personuppgifter behandlas i enlighet med dataskyddsförordningens principer i artikel 5. Möjligheten för personuppgiftsansvarig att säkerställa revision av biträdet ska framgå i PUB-avtal utifrån artikel 28.3 h.

Dataskyddsombudets bedömning

Personuppgiftsansvariga genomför inte någon uppföljning av leverantörer vilket riskerar leda till att artikel 32, säkerhet i samband med behandling inte uppfylls. Vilket val av granskningsmetoder man väljer kan ske utifrån behandlingens art och omfattning, där mindre riskfyllda behandlingar granskas genom att ta del av leverantörers egenkontroll till att de mer riskfyllda behandlingarna granskas genom att se över hur leverantören uppfyller vissa ISO-standarder inom 27000-serien, vad gäller informationssäkerhet. Alternativt anlitar oberoende part som granskar leverantör. Personuppgiftsansvariga bör upprätta rutin för hur man granskar leverantörer, där efter personuppgiftsbehandlingens art och omfattning väljer metod för granskning och regelbundenhet.

Personuppgiftsansvariga saknar en upprättad rutin för ingående av personuppgiftsbiträdesavtal ”PUB-avtal” med personuppgiftsbiträde. I de fall dataskyddssamordnare blivit delaktigt vid upprättande av PUB-avtal har SKR:s mall blivit rekommenderat att användas. I viss utsträckning används personuppgiftsbiträdens förslag till PUB-avtal men om de blivit granskade utifrån dataskyddsförordningen så att de är korrekta och balanserade mellan parterna är inte säkerställt.

Dataskyddsombudet har för granskningen gjort ett urval av dessa PUB-avtal där det ställts mot SKR:s checklista för korrekt upprättade avtal. Syftet med granskningen är inte att granska PUB-avtalen genomgående och anmärka på brister i respektive avtal utan att skapa en överblick av personuppgiftsansvarigas arbete vid ingång av PUB-avtal. Dataskyddsombudet har inte haft möjlighet att granska avtalen utifrån den faktiska arten av personuppgiftsbehandlingen utan enbart utifrån vad som framgår i avtalen; det har inte säkerställts om instruktioner om säkerhetsåtgärder eller vilka personuppgifter som behandlas faktiskt förekommer hos leverantören. Nedanstående brister som iaktagits ger enbart bilden av att det generellt sett finns ett behov av ytterligare kvalitetssäkring inom Sektor Välfärd.

Socialnämnden

Personuppgiftsansvarig bör vid upprättande av personuppgiftsbiträdesavtal säkerställa att ändamål med behandlingen inte enbart hänvisar till att uppfylla tjänsteavtalet, utan ändamålet ska beskriva vilka typer av behandlingar biträdet ska genomföra åt personuppgiftsansvarig. Av vissa PUB-avtal saknas korrekt formalia i form av vem man ingått avtal med samt vilka instruktioner man lämnat till biträde. Ytterligare tycks det vara personer i vissa fall som inte är behörig att underteckna PUB-avtal eller att det saknas underskrift från leverantör. Utifrån ett dataskydd och administrativt perspektiv är det positivt att man i hög utsträckning av de 19 PUB-avtalen använt sig av SKR:s mall för PUB-avtal och uppfyller kraven för ett korrekt PUB-avtal. I viss mån kan instruktioner som lämnats till biträdet vara generiska utifrån exempel i mallen från SKR och om dessa efterlevs av leverantör kan enbart kontrolleras vid en revision av biträde.

Omvårdnadsnämnden

Personuppgiftsansvarig har i hög utsträckning PUB-avtal upprättade före Dataskyddsförordningens ikraftträdande och uppfyller därmed inte kraven på ett korrekt PUB-avtal. Totalt har tre PUB-avtal upprättats efter dataskyddsförordningen ikraftträdande varav för 2 förefaller det inte råda en

biträdessituation. Det tredje PUB-avtalet som är upprättat är efter leverantörens avtalsmall och uppfyller kraven i dataskyddsförordningen.

Arbetsmarknad- och funktionsrättsnämnden

Personuppgiftsansvarig har ett PUB-avtal upprättat med leverantör och uppfyller kraven i dataskyddsförordningen. Övriga avtal med två leverantörer är i egentlig mening inte PUB-avtal utan förefaller vara allmänna villkor om säkerhetsåtgärder för personuppgiftsbehandlingar och bör upprättas på nytt om det föreligger en biträdessituation.

Gemensamt för Sektor Välfärd

Personuppgiftsansvariga bör se över om det råder en biträdesrelation inför upprättande av PUB-avtal, då det i vissa fall verkar som att personuppgiftsansvarig överför personuppgifter till en tjänsteleverantör som sedan behandlar dessa uppgifter i rollen som personuppgiftsansvarig inom sin egen verksamhet, då de bestämmer ändamål och medel för behandlingen.

Avtalsrättsliga aspekter som iakttagits och som personuppgiftsansvariga bör beakta är skadeståndsbegränsningar i avtalen och val av instans i skiljeklausul. Exempelvis om ett skadestånd till registrerade skulle utgå som sedan begränsas till 1 år av kontraktsvärdet samt tvistelösning skulle ske i skiljedomstol kan det leda till en kostsam process.

Processen för PUB-avtal bör beskrivas i rutin för att säkerställa att man i god tid inför upphandling kan säkerställa att man efterlever kraven i artikel 28. Många PUB-avtal har generellt sett upprättats mellan leverantörer och personuppgiftsansvariga kort efter att dataskyddsförordningen trätt i kraft för att säkerställa ett korrekt förfarande. Däremot förekommer det många brister generellt hos flertalet personuppgiftsansvarigas PUB-avtal under Dataskyddsenhetens arbetsområde. Genom säkerställande av rutin bör det leda till att nya PUB-avtal efterlever kraven i artikel 28.

Dataskyddsombudet rekommendation

Upprätta rutin för personuppgiftsbiträdesavtal och granskning av personuppgiftsbiträden.

Granskning av personuppgiftsansvarigas motivering av rättsliga grunder

Behandling av personuppgifter får endast ske under de omständigheter som särskilt anges i förordningen eller i nationell rätt. Behandling ska således vila på en av de rättsliga grunder som framgår av artikel 6 för att den ska vara laglig. I den här granskningen har dataskyddsombudet valt ut tio personuppgiftsbehandlingar ur personuppgiftsansvarigs registerförteckning. Dataskyddsombudet har därefter inhämtat motivering till den rättsliga grunden för att säkerställa att personuppgiftsansvarig använder den korrekta rättsliga grunden.

Vilken grad av tydlighet och precision som krävs i fråga om den rättsliga grunden för att en viss behandling av personuppgifter ska anses vara nödvändig måste bedömas från fall till fall, utifrån behandlingens och verksamhetens karaktär.

En personuppgiftsbehandling som inte utgör någon egentlig kränkning av den personliga integriteten, såsom när det gäller behandling av elevers namn i reguljär skolverksamhet, kan ske med stöd av en rättslig grund som är allmänt hållen. Ett mer kännbart intrång, t.ex. behandling av känsliga personuppgifter inom hälso- och sjukvården, kräver att den rättsliga grunden är mer preciserad och förutsägbart.

Dataskyddsombudets bedömning

Många behandlingar har flera rättsliga grunder och ändamål för en och samma dokumenterad behandling. De rättsliga grunderna kunde kopplas i hög utsträckning till respektive ändamål. Problematiken ligger i att utan motivering för varje rättslig grund upplevs det som otydligt vilken rättslig grund är kopplad till vilket ändamål i behandlingen.

Kopplingen mellan ändamål och rättslig grund visade sig i hög grad vara korrekt. Även om den dokumentation av personuppgiftsbehandlingar uppfyller kraven enligt dataskyddsförordningen upplevs det som otydligt då det enbart med motiveringen av de rättsliga grunderna som det kunde dras en koppling mellan ändamål och rättslig grund.

En ytterligare aspekt som bör beaktas är att med flera rättsliga grunder för en och samma behandling påverkar vilka rättigheter den registrerade får använda sig av enligt artiklarna 15–21. Därav bör behandlingarna delas upp för ökad tydlighet och transparens i registerförteckningen. Personuppgiftsansvariga bör utgå ifrån grundregeln, *en* rättslig grund för *en* behandling.

Motiveringarna till val av rättslig grund vilade på lagstiftning kopplat till respektive verksamhet och i hög utsträckning utgjordes den rättsliga grunden av rättslig förpliktelse, myndighetsutövning och uppgift av allmänt intresse. Motiveringarna gav stöd till att behandlingen i sig är legitim.

Vid ändring av rättslig grund måste även information till registrerade lämnas utifrån informationskravet i dataskyddsförordningen.

Dataskyddsombudet rekommendation

Dela upp behandlingar där det finns flera rättsliga grunder kopplat till olika ändamål.

Fortsätt att dokumentera motivering val av rättslig grund i registerförteckningen.

Uppföljning av 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. Granskningens syfte var att säkerställa att arbetsgivaren är tydlig och transparent över hur de informerar personal om arbetsgivarens personuppgiftsbehandling.

Dataskyddsombudets bedömning

Vid tidigare granskning lämnades rekommendation för vardera fyra områden som dataskyddsombudet granskade vad gäller information om personuppgiftsbehandlingar av anställda. Då tiden mellan denna granskning och tidigare granskning varit kort samt vakanser inom dataskyddsorganisationen har inget åtgärdats. Tidigare rekommendationer kvarstår.

Dataskyddsombudet 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.

Uppföljning av 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

Dataskyddsombudets bedömning

Vid tidigare granskning lämnades rekommendationerna att personuppgiftsansvariga ska genomföra en genomlysning av riskerna för alla deras personuppgiftsbehandlingar samt genomföra konsekvensbedömning om det föreligger hög risk för de registrerades fri- och rättigheter. Då tiden mellan denna granskning och tidigare granskning varit kort samt vakanser inom dataskyddsorganisationen har inget åtgärdats.

Man har fortsättningsvis fortsatt arbetet med att kontinuerligt genomföra konsekvensbedömningar på nya personuppgiftsbehandlingar eller där upphandling av nytt system skett. För att få en systematik i dataskyddsarbete bör genomlysning genomföras för att säkerställa korrekta personuppgiftsbehandlingar enligt dataskyddsförordningen inom hela organisationen. Tidigare rekommendationer kvarstår.

Dataskyddsombudet 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.

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 hade processen förbättrats då från att personuppgiftsincidentenen upptäckts, utredning genomförts och eventuell anmälan skett, har man hållit sig inom tidsramen i högre utsträckning än tidigare år.

För närvarande finns en arbetsgrupp inom Gävle kommun som arbetar för en gemensam portal till olika typer av säkerhetsincidenter vilket personuppgiftsincidenter ingår för att göra det enklare för medarbetare att anmäla incidenter samt att anmäla till rätt personuppgiftsansvarig.

För att personuppgiftsansvariga ska kunna få en översikt över vilka typer av personuppgiftsincidenter som uppstår inom verksamheterna bör man redovisa detta i egen årsredovisning av dataskyddsarbetet för respektive nämnd.

Den bästa åtgärden för att upptäcka och åtgärda personuppgiftsincidenter är fortfarande kontinuerlig utbildning av medarbetare för en god dataskyddskultur.

Dataskyddsombudets rekommendation

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

I tjänsten,

Adrian Vinsa
Dataskyddsombud
Gävle kommuns dataskyddsenhet