Juridik och säkerhet
Dataskyddsombud
Region Västerbotten

Dataskyddsombudets årsrapport 2023

region västerbotten

Innehåll

1. Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU. Enligt dataskyddsförordningen är varje nämnd inom Region Västerbotten ansvarig för att verksamheten följer dataskyddslagstiftningen. Det innebär att nämnder behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter. Varje nämnd har utsett ett Dataskyddsombud (”DSO”). DSO:n har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

I enlighet med artikel 38.3 i dataskyddsförordningen ska DSO rapportera om dataskyddsarbetet till den personuppgiftsansvariges högsta förvaltningsnivå, vilket sker genom denna årsrapport.

2. Sammanfattning och kontrollpunkter

I egenskap av ert Dataskyddsombud, fortsättningsvis kallad DSO, lämnas följande årsrapport.

Under året har DSO genomfört utbildningar under Mars 2023 riktade mot personer med särskilt ansvar för personuppgifter och personuppgiftshandläggare. Under hösten 2023 har dataskyddsombudet haft informationsträff med personuppgiftshandläggarna. Utöver detta genomfört informationsinsatser i mindre grupperingar i särskilda frågor.

Under året har Regionen informerats om två klagomål ställt till IMY angående hanteringen av personuppgifter. IMY har även genomfört en granskning gällande Dataskyddsombudets roll, https://www.imy.se/tillsyner/dataskyddsombudens-roll-och-stallning/ . Det tidigare beslutet om sanktionsavgift på 2,5 miljoner som riktade sig mot behörighetstilldelning i Regionens journalsystem har upphävts genom Kammarrättens dom, https://www.imy.se/tillsyner/region-vasterbotten/. IMY har även i sin tillsynsplan för 2023 (förutom tillsyn grundat på klagomål eller riskbaserad tillsyn) granskat dataskyddsombudets roll. https://www.imy.se/globalassets/dokument/ovrigt/tillsynsplan-2023.pdf. Region Västerbotten har fått besvara frågor kring detta till IMY.

För år 2023 har DSO förutom de fasta kontrollpunkterna även följt upp tidigare genomförda kontroller. De fokusområden som valts ut för 2023 är personuppgiftsbiträdesavtal och registerförteckningen.

Under 2023 har undertecknad varit utsedd som Dataskyddsombud för Regionstyrelsen, Hälso- och sjukvårdsnämnden, Folkhögskolestyrelsen och Regionala utvecklingsnämnden. Kontrollerna genomförs därför för samtliga nämnder gemensamt i denna årsrapport.

Nedan redogörs för den genomförda granskningen och DSO:ns slutsatser samt rekommendationer gällande de kontrollerna som genomförts.

3. Kontrollpunkter

3.1 Uppföljning av tidigare rekommendationer

DSO har tidigare lämnat rekommendationer att nämnderna ska
- registerförteckna alla personuppgiftsbehandlingar
- utse personuppgiftshandläggare
- höja kunskapsnivån gällande rapportering av personuppgiftsincidenter

Registerförteckning

Att föra registerförteckning är ett krav enligt dataskyddsförordningen och ska syfta till att hålla ordning på personuppgiftsbehandlingarna men även tex. kunna uppvisas för tillsynsmyndigheten vid efterfrågan. I Regionen används i nuläget en SharePoint lösning där verksamheterna registrerar sina personuppgiftsbehandlingar. Dataskyddsförordningen ställer krav på vilka uppgifter som ska finnas i registret över personuppgiftsbehandlingar. Det handlar bland annat om ändamål för behandlingen, kategorier av registrerade och huruvida överföring av personuppgifter till tredjeland sker.

Kontroll

Kontrollen sker genom den fördjupade granskningen för året, se sidan 11.

Personuppgiftshandläggare

Verksamhetschefen ansvarar för att utse personuppgiftshandläggare vid enheten. Personuppgiftshandläggarna är en del av Regionens organisation för att säkerställa att kunskapen och resurserna finns för att hantera dataskyddsfrågor på ett korrekt sätt. Personuppgiftshandläggaren skall fungera som verksamhetschefens förlängda arm i dataskyddsfrågor och vara en tydlig kanal in till dataskyddsombudet samt dataskyddsombudets kanal att informera och informera sig. Personuppgiftshandläggaren skall utöver att samråda med dataskyddsombudet i dataskyddsfrågor vid enheten även bistå i att upprätta registerförteckningen och utreda personuppgiftsincidenter samt ta fram de rutiner som behövs vid enheten i dataskyddsfrågor.

Kontroll

Av Regionens dokumentation kring dataskyddets organisation finns beskrivet att en del i dataskyddets organisation är att utse personuppgiftshandläggare. År 2022 har DSO kommenterat att det saknas utsedda personuppgiftshandläggare för flertalet verksamhetsområden. En kontroll i den teamsgrupp som alla personuppgiftshandläggare uppmanas registrera sig har genomförts för 2023.

Utfall av granskningen

Regionstyrelsen

Enligt DSOs årsrapport för 2022 hade Regionstyrelsen utsett 7 st personuppgiftshandläggare för olika verksamheter. För 2023 har Regionstyrelsen utsett 8 st. personuppgiftshandläggare.

Hälso- och sjukvårdsnämnden

Enligt DSOs årsrapport för 2022 hade Hälso- och sjukvårdsnämnden utsett 56 st. personuppgiftshandläggare för olika verksamheter. För 2023 har Hälso- och sjukvårdsnämnden 55 st personuppgiftshandläggare utsedda.

Regionala utvecklingsnämnden

Enligt DSOs årsrapport för 2022 hade Regionala utvecklingsnämnden utsett en personuppgiftshandläggare för nämnden. Regionala utvecklingsnämnden har under 2023 fortsatt en person utsedd som personuppgiftshandläggare.

Folkhögskolestyrelsen

Enligt DSOs årsrapport för 2022 hade Folkhögskolestyrelsen inte utsett personuppgiftshandläggare för nämnden. För 2023 har Folkhögskolestyrelsen anmält 2 st personuppgiftshandläggare.

Kommentar av DSO

Samtliga nämnder har nu utsett personuppgiftshandläggare. Dataskyddsombudet har utifrån det inga synpunkter på antalet utsedda personuppgiftshandläggare. De utsedda personuppgiftshandläggarna är viktiga funktioner för att ett aktivt arbete med efterlevnad av GDPR genomförs i verksamheterna och en viktig del i att sprida kunskap i verksamheten. Beroende på området personuppgiftshandläggaren arbetar inom (hur mycket personuppgifter som hanteras, känslighet och hur många verksamheter det gäller) behöver också personuppgiftshandläggarens resurser säkerställas.

Personuppgiftsincidenter

En personuppgiftsincident definieras som en säkerhetsincident som leder till oavsiktlig eller olaglig, förstöring, förlust, ändring, obehörigt röjande av eller obehörig åtkomst till de behandlade personuppgifterna. Alla personuppgiftsincidenter skall dokumenteras och om incidenten kan leda till att de registrerade utsätts för allvarliga risker, måste Integritetsskyddsmyndigheten underrättas inom 72 timmar från upptäckten.

Kontroll

Dataskyddsombudet uppmärksammade i årsrapporten för 2022 att personuppgiftsincidenter rapporterats för HSN och RS medan både RUN och FHS saknade rapporterade incidenter. RS bedömdes även rapporterat en låg mängd incidenter särskilt då CIMT ligger under RS. Dataskyddsombudet har därför följt upp mängden inrapporterade incidenter för år 2023 samt ställt frågor till de verksamheter som helt saknar incidenter (RUN, FHS samt verksamhetsområden inom RS).

Utfall av kontrollen

För 2023 har HSN rapporterat 24 st Personuppgiftsincidenter, RS 9st och både RUN och FHS saknar även för 2023 inrapporterade incidenter (2023-01-01- 2023-11-15). Utifrån detta resultat har dataskyddsombudet ställt kompletterande frågor till RS, RUN och FHS hur rapportering av personuppgiftsincidenter har implementerats i verksamheten.

FHS beskriver att de upplever att de saknar kunskap och resurser för arbetet. Det är således inte känt i verksamheten vad som utgör en personuppgiftsincident och hur dessa rapporteras.

RUN beskriver att det skett en (1) incident under 2023 som skall vara inrapporterad men saknas i Platina. Enligt personuppgiftshandläggaren vid RUN ska det om det upptäcks en personuppgiftsincident rapporteras genom att fylla i Regionens avvikelseblanketten och skickar denna till RUF:s personuppgiftshandläggare. Personuppgiftshandläggaren ansvarar för vidare utredning kring personuppgiftsincidenten och informerar RUF:s ledning /Regional utv. direktör. Nya medarbetare och praktikanter vid RUN får information om vad man gör vid personuppgiftsincidenter samt riktlinjer kring GDPR. Det sker i samband med inskolning för nyanställda samt i introduktionen praktikanter.

DSO har även ställt frågan till RS enhet CIMT där förväntan av rapporterade incidenter varit högre än statistiken visar. En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter. Inom CIMT skulle en sådan incident t.ex. kunna utgöras av borttappade eller stulna datorer, utpressnings eller dataexfiltreringsattacker. DSO har i detta syfte vänt sig till verksamheterna för att förhöra sig om hur den här typen av incidenter hanteras inom CIMT. Svar från verksamheten är att säkerhetsansvarige hanterar incidenter samt att verksamheterna själva hanterar felaktiga uppgifter i journaler och liknande incidenter.

Kommentar av DSO

Det är alltid svårt att enbart på mängden inrapporterade incidenter avgöra om brister föreligger. En låg mängd incidenter kan antingen tyda på att verksamheten inte uppmärksammar incidenter eller att incidenter inte inträffar. Dataskyddsombudet kan således inte utifrån antalet incidenter uttala sig.

Dataskyddsombudet kan konstatera att FHS inte bedriver ett aktivt arbete enligt GDPR. Detta arbete behöver påbörjas och incidenter behöver rapporteras om sådana uppstår.

RUN har under året haft en incident som rapporterats utan att diarieföras. Detta behöver åtgärdas. I övrigt finns det tydliga rutiner för rapportering av personuppgiftsincidenter inom verksamheten samt ett aktivt arbete med frågan.

RS har i samband med föregående årsrapport skrivit att nämnden ska säkerställa deltagandet av de planerade utbildningar som ska genomföras enligt Dataskyddsombudets kontrollplan för granskning av verksamheternas dataskyddsarbete 2023. CIMT har en egen upprättad Checklista vid anmälan om personuppgiftsincident[1]. Rutiner för hanteringen av incidenter finns alltså på plats. DSO kan konstatera att det torde finnas avvikelser gällande tex. borttappade eller stulna datorer/mobiltelefoner tex. dessa avvikelser saknas. Om dessa personuppgiftsincidenter skulle rapporterats av CIMT eller av verksamheten (tex. HSN) framgår inte av rutinerna eller svaret från verksamheten. Hanteringen av t.ex. nätfiske och incidenter på detta område ska hanteras av säkerhetsansvarig, det är oklart av svaret från verksamheten

[1] https://vlladmin.sharepoint.com/sites/ledningssystem-it/Faststllda%20dokument/Checklista%20vid%20anm%C3%A4lan%20om%20personuppgiftsincident(307839).pdf

om incidenter inte skett eller om dessa inte rapporterats i Platina. Ekonomi, HR och andra personuppgiftstunga verksamheter ligger även under RS.

Objektet Ärende- och dokumenthantering har under året även uppmärksammats på att de avvikelser som rapporteras i modulen taggas med uppgiften ”personuppgiftsincidenter” och ”GDPR”. Detta i sig är inget problem, utifrån taggning sågs dock en risk att dessa inte utreddes enligt rutin (diarieföring och utredning i diariet via manuell rutin). En stickprovskontroll har genomförts som visar att det finns avvikelser i avvikelsesystemet som inte har utretts internt som personuppgiftsincidenter. Typen av personuppgiftsincidenter som kommit upp vid stickprovskontrollen har dock inte utgjort den typen av personuppgiftsincidenter som personuppgiftsansvarige även behöver rapportera till tillsynsmyndigheten IMY inom 72h. Dataskyddsombudet har lämnat rekommendationer att verksamheterna bör gå igenom de avvikelser som har klassificerats som ”personuppgiftsincident” och ”informationssäkerhet” under föregående år och kontrollera ifall det finns personuppgiftsincidenter som enbart rapporterats in som en avvikelse. Har detta skett ska dessa också rapporteras in som personuppgiftsincidenter. Vid en kontroll finns avvikelser kvar i systemet utan koppling till diarieförda ärenden.

Sammanfattningsvis anser DSO att det finns risker med de upprättade rutinerna för rapporteringen av personuppgiftsincidenter utifrån utebliven rapportering. Risken är att händelser i verksamheten inte rapporteras som personuppgiftsincidenter utan enbart som tex. medicinska avvikelser (vid dokumentation i fel journal) eller serviceavvikelser (vid borttappade mobiltelefoner) eller säkerhetsavvikelser (vid externa attacker). Det behöver säkerställas att personuppgiftsincidenter som rapporteras som andra incidenter tas ställning till utifrån GDPRs bestämmelser (exvis informera de registrerade eller tillsynsmyndighet). Ansvarsfördelningen för de olika typerna av incidenter behöver tydliggöras för att säkerställa att incidenter som sker i verksamheterna även bedöms utifrån GDPRs bestämmelser.

3.2 Fasta kontrollpunkter

Kontrollpunkt 1: Styrdokument för dataskyddsarbetet

Kontrollpunkten avser verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete, och omfattar bland annat verksamhetens dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt tillhandahållna resurser för arbetet.

Kontroll

Dataskyddsombudet har gått igenom de ledningssystemsdokument som finns gällande regionens dataskydd som återfinns i ledningssystemet.

Utfall av kontroll

I ledningssystemet återfinns styrande och ledande dokument som beskriver stora delar av hanteringen enligt GDPR. Det område som saknar ledning och styrning är delar kring hur Regionen tillgodoser de enskildas rättigheter.

Kommentar av DSO

Alla nämnder behöver säkerställa att rutiner finns för att hantera de enskildas rättigheter.

Kontrollpunkt 2: Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

Kontrollpunkten avser regionens förmåga att säkerställa att tekniska och organisatoriska åtgärder vidtas till skydd för personuppgifterna. Regionen ansvarar för att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda de personuppgifter som behandlas. Vilka säkerhetsåtgärder som är lämpliga beror bland annat på hur känslig behandlingen är, vilka risker som finns för de anställda och vilka tekniska lösningar som är tillgängliga. Exempel på tekniska säkerhetsåtgärder är inloggning, behörighetsspärrar, brandväggar, kryptering, pseudonymisering, säkerhetskopiering och antivirusskydd. Organisatoriska säkerhetsåtgärder handlar om det administrativa säkerhetsarbetet som till exempel tilldelning av åtkomsträttigheter, interna rutiner, instruktioner och riktlinjer.

Kontroll

För att säkerställa att rätt tekniska åtgärder vidtas är klassning av information en del i arbetet. Detta ger verksamheterna ett stöd i att fatta rätt beslut utifrån säkerhet. Dataskyddsombudet har därför bett att få ta del av fyra klassningar som genomförts 2023.

Utfall av kontrollen

De fyra klassningarna DSO har tagit emot har beskrivningar kring åtgärder som skall vidtas och handlingsplan för detta.

Kommentar av DSO

DSO har saknat resurser att granska om tekniska och organisatoriska åtgärder som angetts i KLASSA verktyget faktiskt har åtgärdats och kommer istället att återkomma till detta under 2024.

Kontrollpunkt 3: Personuppgiftsincidenter

Kontrollpunkten avser verksamhetens förutsättningar att identifiera och hantera personuppgiftincidenter. För att uppfylla ansvarsskyldigheten bör verksamhetens rutin för hanteringen vara dokumenterad. I de fall verksamheten är både personuppgiftsansvarig och personuppgiftsbiträde bör rutinen omfatta båda scenarier. I kontrollpunkten ingår även översyn av verksamhetens rutin för att bedöma incidenten, hantering av eventuell anmälan till tillsynsmyndigheten samt hur rutinerna tillgängliggörs och kommuniceras inom verksamheten. Även efterlevnad av verksamhetens dokumentationsskyldighet, att alla inträffade personuppgiftsincidenter registreras, innefattas.

Kontroll

Kontrollen genomfördes inom uppföljning av tidigare rekommendationer, se sidan 5.

Kontrollpunkt 4: Personuppgiftbiträdesavtal

Kontrollpunkten avser verksamhetens dokumentation av biträdesavtal och andra överenskommelser gällande dataskydd, och förutsätter att verksamheten har identifierat samt registrerat personuppgiftsbiträden i registerförteckningen. Även verksamhetens rutiner för uppdatering och uppföljning av tecknade biträdesavtal innefattas.

Kontroll

Kontrollpunkten hanteras i den fördjupade granskningen för år 2023, se sidan 10.

Kontrollpunkt 5: Registerförteckning

Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även verksamhetens arbete med, och rutin för, att säkerställa ett uppdaterat och heltäckande personuppgiftsregister innefattas.

Kontroll

Kontrollpunkten hanteras i den fördjupade granskningen för år 2023, se sidan 11.

Kontrollpunkt 6: Konsekvensbedömning/samråd

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras samt genomföra denna. Även verksamhetens rutiner för arbetet med konsekvensbedömningar samt hur dataskyddsombudet involveras i arbetet ingår. Därtill tillkommer verksamhetens rutin för att hantera de risker som identifieras i konsekvensbedömningen, samt hur genomförda konsekvensbedömningar följs upp och hålls aktuella.

Kontroll

Dataskyddsombudet har sökt i diariet efter genomförda konsekvensbedömningar.

Utfall av kontroll

Dataskyddsombudet hittar inga diarieförda konsekvensbedömningar under 2023. Dataskyddsombudet finner en tröskelanalys som landat i att konsekvensbedömning inte behöver genomföras. Det finns rutiner och mallar för konsekvensbedömningar och dessa beskrivs även i ledningssystemet. [2]

Kommentar av DSO

Att verksamheterna genomför och diarieför konsekvensbedömningar är en viktig del i att analysera nya personuppgiftsbehandlingar i verksamheten. DSO ser att

[2] https://vlladmin.sharepoint.com/sites/ledningssystem-ledningsstaben/Faststllda%20dokument/Konsekvensbed%C3%B6mning%20avseende%20dataskydd.pdf

Regionen har bedrivit ett arbete under året gällande rutiner för när konsekvensbedömningar skall genomföras och dataskyddsombudet finns även som rådgivande vid upprättandet av konsekvensbedömningarna[3]. DSO har inte genomfört en djupare analys om avsaknaden av konsekvensbedömningar är rimlig eller ej.

Kontrollpunkt 7: Hantering av registrerades rättigheter

Kontrollpunkten avser verksamhetens förutsättningar för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering. En förutsättning för att verksamheten ska kunna hantera de registrerades rättigheter är att det finns en process och rutiner för arbetet, så att den registrerades personuppgifter enkelt kan lokaliseras vid efterfrågan.

Kontroll

DSO har sökt i diariet efter inkomna förfrågningar gällande utövandet av rättigheter enligt GDPR.

Utfall av kontroll

Regionen har tagit emot 1 förfrågan om registerutdrag under 2023 vid en sökning i diariet.

Kommentar av DSO

DSO har tagit emot frågor gällande främst kostnadsfrågan av registerutdrag av olika verksamheter under året. Det är oklart om dessa frågor resulterat i en begäran av en enskild. Om så är fallet har begäran inte diarieförts. Det saknas rutiner i ledningssystemet för att hantera enskildas begäran. Regionen har inte tagit emot klagomål kring de enskildas rättigheter.

Sammanfattningsvis är det viktigt att det finns rutiner ute i verksamheten för hantering av begäran om enskildas rättigheter. DSO kommer att följa upp denna punkt.

Kontrollpunkt 8: Kunskapsnivån i verksamheten

Kontrollpunkten avser verksamhetens arbete med att utbilda och upprätthålla kunskapsnivån i dataskyddsfrågor hos anställda.

Kontroll

En enkät har gått ut riktad till personuppgiftshandläggare gällande kunskaper om GDPR.

En enkät har gått ut riktad till verksamhetschefer gällande kunskaper om GDPR.

Utfall av kontroll

Ungefär hälften av de tillfrågade personuppgiftshandläggarna anser att de har nog kunskap om GDPR för att utföra sitt uppdrag som personuppgiftshandläggare. Majoriteten av de som anser att de har bristfälliga kunskaper anger att de saknar kunskap om registerförteckningen och laglig grund.

[3] https://vlladmin.sharepoint.com/sites/ledningssystem-ledningsstaben/Faststllda%20dokument/Anskaffning,%20utveckling%20och%20f%C3%B6r%C3%A4ndring%20av%20informationssystem.pdf

Ungefär hälften av de tillfrågade cheferna anser att de har tillräcklig kunskap om GDPR i rollen som chef. Majoriteten uppger även att de har kunskap om personuppgiftsincidenter och registerförteckningar. Hälften av de tillfrågade cheferna har varit i kontakt med dataskyddsombudet för råd och stöd i GDPR frågor.

Kommentar av DSO

DSO har haft utbildningar för personuppgiftshandläggare och nätverksträffar under året. DSO kommer inför nästkommande nätverksträffar under hösten och våren 2024 att använda underlaget i undersökningen för att rikta utbildningarna på de områden personuppgiftshandläggarna själva angett de saknar kunskap inom.

3.3 Fördjupad kontroll 2023

Personuppgiftsbiträdesavtal

Den personuppgiftsansvarige är ansvarig för all personuppgiftsbehandling som utförs å dennes vägnar. En personuppgiftsansvarig som anlitar ett personuppgiftsbiträde att utföra personuppgiftsbehandlingar för sin räkning kan inte avsäga sig de skyldigheter som följer av detta ansvar. Det är således av stor vikt att personuppgiftsansvariga har överblick över sina anlitade personuppgiftsbiträden och att de uppfyller de kvalitetskrav och krav vid, bl.a., anlitande av underbiträden som uppställs i förordningen. Förordningen kräver även att förhållandet mellan den personuppgiftsansvarige och personuppgiftsbiträdet regleras genom avtal (eller annan rättsakt). Förordningen uppställer även vissa krav på vad ett sådant avtal ska innehålla. Denna fördjupade kontroll syftar till att undersöka vilka som behandlar personuppgifter för Region Västerbottens räkning och ifall dessa förhållanden är reglerade genom adekvata avtal.

Kontroll

Av rutinerna Regionen har framgår att Personuppgiftsbiträdesavtal skall diarieföras i Platina samt att SKRs mall för biträdesavtal skall användas. Dataskyddsombudet har valt ut de leverantörer som tillhandahåller teknikkomponenter enligt objektförvaltningen i vårdstöd bas skall granskas. Detta innefattar systemen Pascal, Cytodos, Exorlive, Picsara, NCS Cross, CGM 14, PMO, Voxit Vocal, Obstetrix/Milou, Prator. Frågan har ställts till objektförvaltningen om dessa leverantörer har Personuppgiftsbiträdesavtal tecknade med regionen.

Utfall av kontrollen

NCS Cross, EyeDoc, Cytodos, Metavision, Obstetrix samt Prator har ett PuB-avtal tecknat som följer SKRs mall och är diarieförda i diariet.

När det gäller CGMJ4 samt Picsara så pågår arbetet med att teckna avtal i dagsläget finns dock inga diarieförda avtal.

När det gäller Voxit Vocal samt PMO saknar Personuppgiftsbiträdesavtal då leverantören inte hanterar personuppgifter för Regionens räkning enligt objektförvaltningen. När det gäller Exorlive saknas PuB-avtal i diaret. DSO har inte lyckats komma i kontakt med någon inom förvaltningen som känner till systemet utifrån frågeställningen.

Kommentar av DSO

Att teckna Personuppgiftsbiträdesavtal är en kritisk del i att använda biträden för hanteringen av Regionens personuppgifter. Stickprovskontrollen visar att det i vissa fall saknas personuppgiftsbiträdesavtal, detta är allvarligt och behöver åtgärdas skyndsamt. Att inte teckna personuppgiftsbiträdesavtal med leverantörer är förutom ett brott mot GDPR även en säkerhetsrisk. DSO uppmanar samtliga verksamheter att se över personuppgiftsbiträdesavtalen men även att diarieföra de avtal som har tecknats. DSO har vid kontrollen haft återkommande problem att återfinna avtal som tecknats. DSO kommer att göra stickprovskontroller även kommande år i denna fråga.

Registerförteckningen

Registerförteckningen är ett krav enligt dataskyddsförordningen och ska även kunna uppvisas för tillsynsmyndigheten vid efterfrågan. I Regionen används i nuläget en sharepointlösning där verksamheterna registrerar sina behandlingar. Dataskyddsförordningen ställer krav på vad som ska förekomma i registret över personuppgiftsbehandlingar. Det handlar bland annat om ändamål för behandlingen, kategorier av registrerade och huruvida överföring av personuppgifter till tredjeland sker. Denna fördjupade kontroll avser undersöka Regionens dokumentation av personuppgiftsbehandlingarna för att säkerställa att de krav som förordningen ställer upp efterlevs.

Kontroll

Dataskyddsombudet har kontrollerat antalet registerförteckningar som har tillkommit eller redigerats under 2023 för samtliga nämnder samt genomfört en stickprovskontroll på 5 förteckningar per nämnd med syfte att kontrollera om dessa är korrekt ifyllda.

Utfall av kontrollen

RUN, HSN och RS har lagt till eller uppdaterat registerförteckningen under året. FHS saknar fortfarande registerförteckningar i systemet.

Utfallet av stickprovskontrollerna vid HSN, RS samt RUN visar att de inskickade registerförteckningarna i stort var godtagbara, de obligatoriska uppgifterna framgick i de allra flesta förteckningarna. Dock fanns det frågetecken kring om rätt rättslig grund angetts. Detta har dock kommenterats av DSO och kommer åtgärdas av personuppgiftshandläggaren.

Då FHS saknar registerförteckningar har inga stickprovskontroller varit möjliga att genomföra.

Kommentar av DSO

En kontroll vid inskickande av förteckningarna vore att föredra. DSO har inte haft utrymme att kontrollera inskickade förteckningar. Rekommendationen till verksamheterna är att hitta rutiner för att årligen uppdatera förteckningarna. DSO kommer att genomföra en utökad stickprovskontroll under kommande år i syfte att hjälpa verksamheterna med utformningen av förteckningarna.

4. DSOs sammanfattande rekommendationer

DSO har lämnat rekommendationer för varje punkt som kontrollerats ovan. Utöver dessa specifikt riktade rekommendationerna vill DSO även lyfta fram generella rekommendationer utifrån de observationer som har gjorts för år 2023.

- Varje personuppgiftsansvarig har en ansvarsskyldighet. Denna ansvarsskyldighet innebär en skyldighet att kunna visa att dataskyddsförordningen uppfylls. Det är utifrån detta otroligt viktigt att ha kontroll över de personuppgiftsbehandlingar som sker inom personuppgiftsansvariges område och förteckna dessa samt de omständigheter som finns kring personuppgiftsbehandlingarna såsom personuppgiftsincidenter, tredjelandsöverföringar eller konsekvensbedömningar. DSO rekommenderar samtliga nämnder att ta fram rutiner för denna typ av dokumentation.
- Kunskapen inom verksamheterna gällande GDPR behöver generellt förbättras, en plan för utbildning av anställda och andra nyckelpersoner rekommenderas.

Umeå 12-01-2023

Josefin Leijon

Dataskyddsombud