Grundskolenämnden
Barn- och utbildningsförvaltningen
Kvalitetsenheten
Per Silvervret Boberg 016-710 45 02

Datum
2024-04-03

Diarienummer
GSN/2024:107

Handlingsnummer
2024:981

Grundskolenämnden

Förslag till beslut - Svar på dataskyddsombudets årsrapport 2023 för dataskydd för grundskolenämnden

Förslag till beslut

Svaret antas och översänds till dataskyddsombudet.

Ärendebeskrivning

En av dataskyddsombudets (DSOs) uppgifter är att övervaka efterlevnaden av dataskyddslagarna åt nämnderna och rapportera till nämnderna minst en gång per år. Utifrån denna uppgift har DSO inkommit med en årsapport 2023 för dataskydd för nämnden, vilken för 2023 omfattade en kontroll av grundläggande krav och förutsättningar för att efterleva dataskyddsförordningen:

- Nämndens dataskyddsorganisation
- Registerförteckning
- Personuppgiftsbiträdesavtal
- Personuppgiftsincidenter
- Utbildning i dataskydd för personal
- Konsekvensbedömningar (DPIA)

Resultatet baseras på kontroller som genomfördes under hösten 2023 via frågeformulär och viss dialog. Förändringar kan därför ha skett efter det. Resultatet baseras även på DSO:s observationer under året.

Nämndens svar redovisas per ämnesområde utifrån DSO:s presenterade resultat och rekommendation.

Grundskolenämndens svar

Nämndens dataskyddsorganisation

Resultat

Nämnden har tillgång till stöd av dataskyddsombud och dataskyddssamordnare och uppfyller därmed lagkrav och kommunens styrande dokument. Under […] hösten 2023 [har] det skett en förbättring i form av utökad dataskyddsorganisation.

Rekommendation
Då det behövs mycket stöd i dataskyddsarbete både för att upprätthålla grunddokumentation, hantera incidenter och i samband med upphandlingar och digitalisering behöver nämnden bevaka detta så att brist på stöd inte blir ett hinder i digitaliseringsarbete och annat dataskyddsarbete, och att man utökar vid behov.

Kommentar
Som DSO noterar har arbetet förbättrats i form av en utökad dataskyddsorganisation. Arbetet med dataskydd finansieras inom ram. En tjänst på förvaltningskontoret samordnar dataskydds-, informationssäkerhets- och informationsförvaltningsarbete. Nämnden bevakar stöd och resurser, och signalerar i behov och prioriteringar om resurserna skulle bli otillräckliga.

Registerförteckning (Artikel 30)

Resultat
Nämnden har en registerförteckning men det är oklart om den är fullständig. Ett arbete med inventering av personuppgiftsbehandlingar och uppdateringar av registerförteckning planeras. Uppdatering sker även kontinuerligt när nya behandlingar av personuppgifter tillkommer.

Rekommendation
Min rekommendation är inventering och komplettering sker enligt plan så att dokumentationen i registerförteckningen uppfyller minst minimumlagkrav då en komplett registerförteckning är en förutsättning för att ha ordning på sina personuppgiftsbehandlingar och att tillgodose de registrerades rättigheter, t ex när de registrerade begär registerutdrag över sina personuppgifter enligt artikel 15. De fält som minst ska fyllas i enligt dataskyddsförordningen är följande:

- Namn och kontaktuppgifter för den personuppgiftsansvariga, den personuppgiftsansvarigas företrädare samt dataskyddsombudet.
- Ändamålen med behandlingen.
- En beskrivning av kategorierna av registrerade och kategorierna av personuppgifter.
- De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut.
- I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation.
- Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter. Ej enbart hänvisning till informationshanteringsplan utan de faktiska tidsfristerna.
- Om möjligt, en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder.

Dessa fält är obligatoriska och måste vara korrekt ifyllda för att lagkrav ska uppfyllas. Även informationen i de frivilliga fälten ska enligt dataskyddsförordningen finnas dokumenterad någonstans och det är därför en fördel att även fylla i de dessa så att informationen finns samlad.

Samtliga typer av personuppgiftsbehandligar behöver bli identifierade. Utöver de behandlingar som finns i olika IT-system behöver även de behandlingar som förekommer i t ex e-post, system för digitala möten, samarbetsytor, kontorsprogram, appar och sociala medier mm identifieras. Dessa behöver även gås igenom för att se om det finns några som behöver avslutas.

Det finns en mall i kommunen för alla nämnder att använda och en instruktion för hur fälten fylls i.

Kommentar
Nämnden instämmer i att dess registerförteckning behöver förbättras och kompletteras. Detta arbete har påbörjats med att en inventering av personuppgiftsbehandlingar har genomförts i samband med genomgång av skolnämndernas informationshanteringsplaner under hösten 2023/Q1 2024. Denna inventering kommer att kompletteras med en förfrågan under hösten 2024 till samtliga verksamheter via rektorer och chefer om att komplettera med nya och existerande personuppgiftsbehandlingar.

Personuppgiftsbiträdesavtal (Artikel 28 och 5)

Resultat
Det saknas i vissa fall personuppgiftsbiträdesavtal med leverantörer som behandlar personuppgifter för nämndens räkning. Hur många som saknas är inte känt.

Rekommendation
Min rekommendation är att de personuppgiftsbehandlingar som saknar personuppgiftsbiträdesavatal identifieras och att det säkerställs att de har giltiga och adekvata personuppgiftsbiträdesavtal med instruktioner till biträdet och lista på underbiträden samt att man har säkerställt att underbiträdena är lämpliga. Detta behöver göras skyndsamt då avsaknad av personuppgiftsbiträdesavtal är en risk för både de registrerade personerna som omfattas av behandlingen och för nämnden då det inte finns kontroll över hur personuppgifterna behandlas av leverantörerna.

Kommentar
Nämnd genomgång av samtliga personuppgiftsbehandlingar identifierar också om personuppgiftsbiträdesavtal saknas med någon leverantör. Översynen av befintliga personuppgiftsbiträdesavtal pågår och tecknande av nya personuppgiftsbiträdesavtal sker löpande med prioritet till de största avtalen först. Samverkan med upphandlingsenheten sker också för att säkerställa att existerande avtal och nya avtal uppfyller dataskyddskraven. Samarbetet med upphandlingsenheten underlättar också att nämnden följer lagkrav vad gäller aktiva sanktioner mot Ryssland och Belarus samt Lagen om offentlig upphandling. Arbetet med personuppgiftsbiträdesavtal är långsiktigt och också kontinuerligt i och med revideringar som sker och kan därför inte tidsättas.

Personuppgiftsincidenter (Artikel 33)

Resultat
De incidenter som rapporteras dokumenteras, till exempel så ska anmälan till IMY sparas. Vissa brister finns på området till exempel vad gäller om alla incidenter dokumenteras korrekt och om vissa delar som behöver dokumenteras finns med. Stöddokument för dokumentation finns och utveckling av dessa är planerade.

Under 2023 har nämnden haft 27 personuppgiftsincidenter, varav 19 har anmälts till IMY.

Incidenter som inte anmäls till IMY förs in i en förteckning.

Dataskyddsombudet rådfrågas och hålls vid behov uppdaterad löpande under arbetet med vissa incidenter. När det gäller mindre incidenter eller incidenter som är repetitiva informeras dataskyddsombudet i vissa fall.

Följande brister när det gäller personuppgiftsincidenter förekommer hos nämnden:

- I nuläget rapporteras troligen inte alla incidenter in från verksamheterna.
- Det förekommer att incidenter rapporteras in sent från verksamheterna.
- Dokumentation är inte komplett och saknar i vissa fall t ex riskanalys eller vissa åtgärder.

Rekommendation
Mina rekommendationer är följande:
- Att information ges till verksamheterna så att incidenter rapporteras in och att de rapporteras in direkt när de händer.
- Att personuppgiftsincidenter dokumenteras enligt krav.

Kommentar
Som DSO nämner rådfrågas DSO vid incidenter av icke repetitiv karaktär. Den vanligaste typen av incident är borttappade eller stulna digitala enheter, vars anmälningar ofta har en repetitiv karaktär.

En digital utbildning kring hur man anmäler en personuppgiftsincident (Personuppgiftsincident… Vad är det?) har tagits fram av dataskyddssamordnare på Serviceförvaltningen. Utbildningen riktar sig till hela kommunen. Utbildningen kring hur man anmäler en personuppgift görs obligatoriskt för barn- och utbildningsförvaltningens medarbetare att genomföra under Q2-Q4 2024.

Dokumentationen av incidenter av icke repetitiv karaktär sker nu med stöd av de mallar som nämns.

Utbildning i och information om dataskydd för personal

Resultat
Kommunen har en digital grundutbildning i dataskydd sedan flera år tillbaka som alla medarbetare kan ta del av men som inte är obligatorisk.

Alla medarbetare ska ha fått en grundläggande information om GDPR och under perioden 220901 – 230831 har vissa utbildningsinsatser gjorts efter önskemål samt att medarbetare informerats om att det finnsmöjlighet att delta i utbildning.

Rekommendation
Mina rekommendationer är följande:

- Att det blir obligatoriskt för alla att gå en utbildning, t ex en digital utbildning för att öka förståelsen och kompetensnivån allmänt i organisationen. Även de som gick för några år sedan behöver gå igen.
- Att vissa roller får en fördjupad utbildning eller en riktad utbildning för just den funktionen.

Kommentar
Den grundläggande utbildningen i dataskydd görs obligatorisk för barn- och utbildningsförvaltningens medarbetare att göra under 2025.

Riktad kompetensutveckling i dataskydd för nyckelroller på barn- och utbildningsförvaltningen, såsom skoladministratörer, intendenter samt stöd- och ledningsfunktioner erbjuds löpande av dataskyddssamordnare utifrån identifierade behov.

Konsekvensbedömningar (DPIA) (Artikel 35)

Resultat
Arbetet med konsekvensbedömningar går framåt trots att de är tidskrävande och att det är en utmaning att dokumentera tillräckligt, bedöma risker och ta fram åtgärder. De görs inte alltid när det finns krav utan prioriteringar har gjorts utifrån resurser då de är tidskrävande.

Under perioden 220101 – 230831 har 7 konsekvensbedömningar gjorts antingen slutförts eller påbörjats.

Dataskyddsombudet rådfrågas oftast inför konsekvensbedömningar och ombeds att granska och bedöma laglighet när konsekvensbedömningen bedöms vara klar.

Det finns vissa brister:

- Det saknas vissa konsekvensbedömningar.
- Dokumentationen är i vissa fall något knapphändig.
- Det finns fall där dataskyddsombudets råd inte har följts. Motivering har dock dokumenterats.

Rekommendation
Mina rekommendationer är att nämnden:

- Utför de konsekvensbedömningar som saknas.
- Säkerställer att beskrivningarna är tillräckligt tydliga så att en utomstående förstår behandlingen och hur den kommer att hanteras.

Kommentar
Den nämnda genomgången av personuppgiftsbehandlingar samt översynen av befintliga personuppgiftsbiträdesavtal underlättar identifieringen av var konsekvensbedömningar behöver göras. Likt hur befintliga behov av personuppgiftsbiträdesavtal hanteras behöver genomförandet av konsekvensbedömningar prioriteras efter ärendets dignitet. Förvaltningen kommer också att förtydliga dokumentationen för att göra den mer tillgänglig.

———

Beslutet skickas till:
Dataskyddsombudet
Akten

BARN- OCH UTBILDNINGSFÖRVALTNINGEN

Lina Axelsson Kihlblom
Förvaltningschef

Cathrine Olsson
Administrativ chef

Dataskyddsombudets årsrapport för 2023 för dataskydd för Grundskolenämnden

Denna rapport gäller dataskydd inom vissa utvalda delar av dataskyddsområdet för Grundskolenämnden. Den ger ingen komplett bild av dataskyddet hos nämnden. Årsrapporten innehåller resultatet av kontroller och observationer.

Sammanfattning

Under 2023 utfördes kontroller inom följande områden:

- Nämndens dataskyddsorganisation
- Registerförteckning
- Personuppgiftsbiträdesavtal
- Personuppgiftsincidenter
- Utbildning i dataskydd för personal
- Konsekvensbedömningar (DPIA)

Kontrollerna visade att:

- Nämnden har den **dataskyddsorganisation** som föreskrivs i kommunens Anvisningar för behandling av personuppgifter. En utökning har skett under hösten 2023.
- Nämnden har en **registerförteckning** men det är oklart om den är fullständig.
- Det saknas i vissa fall **personuppgiftsbiträdesavtal** med leverantörer som behandlar personuppgifter för nämndens räkning. Hur många som saknas är inte känt.
- Under perioden 220901 – 230831 har nämnden haft 27 personuppgiftsincidenter varav 19 har anmälts till IMY. Det finns vissa brister som rör hanteringen av **personuppgiftsincidenter**, så som brister i dokumentationen och att dataskyddsombudet inte involveras enligt lagkrav. Verksamheterna jobbar annars på det stora hela bra med sina incidenter.
- Det finns en digital **utbildning** i grundläggande GDPR och en ny i identifiering av personuppgifter. Alla medarbetare ska ha fått en grundläggande information om GDPR och under perioden 220901 – 230831 har vissa utbildningsinsatser gjorts efter önskemål.

- Arbetet med **konsekvensbedömningar** går framåt trots att de är tidskrävande. De görs inte alltid när det finns krav utan prioriteringar har gjorts utifrån resurser då de är tidskrävande. Under perioden 220101 – 230831 har 7 konsekvensbedömningar antingen slutförts eller påbörjats.

Mina rekommendationer är följande:

- Då det behövs mycket **stöd i dataskyddsarbete** både för att upprätthålla grunddokumentation, hantera incidenter och i samband med upphandlingar och digitalisering behöver nämnden bevaka detta så att brist på stöd inte blir ett hinder i digitaliseringsarbetet och att man utökar vid behov.
- Att nämnden säkerställer att **registerförteckningarna** kompletteras och uppdateras då kompletta registerförteckningar är en förutsättning för att ha ordning på sina personuppgiftsbehandlingar och att tillgodose de registrerades rättigheter.
- Att de personuppgiftsbehandlingar som saknar **personuppgiftsbiträdesavatal** identifieras och att det säkerställs att de har giltiga och adekvata personuppgiftsbiträdesavtal med instruktioner till biträdet och lista på underbiträden samt att man har säkerställt att underbiträden är lämpliga.
- Att nämnden informerar verksamheterna så att **personuppgiftsincidenter** rapporteras in och att dokumentationen av incidenterna förbättras och att dataskyddsombudet involveras.
- Att **utbildningsinsatser** görs för medarbetare och chefer. Att det blir obligatoriskt för alla att gå en utbildning i dataskydd för att öka förståelsen och kompetensnivån allmänt i organisationen och för att höja statusen på dataskydd. Att vissa roller får en fördjupad eller riktad utbildning.
- Att konsekvensbedömningar görs för de behandlingar som behöver enligt lag men saknar idag samt att dokumentation förbättras i **konsekvensbedömningarna**.

Innehåll

Dataskyddsförordningen

EU:s dataskyddsförordning (GDPR) gäller som lag i samtliga EU-länder, inklusive Sverige. Den har sina rötter i Europakonventionen om de mänskliga rättigheterna och finns till för att skydda enskildas (de registrerades) grundläggande rättigheter och friheter, särskilt deras rätt till privat- och familjeliv, inklusive arbetslivet, och skydd av personuppgifter. Syftet är även att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter så att det fria flödet av uppgifter inom Europa inte hindras.

Varje behandling av personuppgifter behöver uppfylla dataskyddsförordningen och dess grundläggande principer. Dessa är i korthet att personuppgiftsansvarig:

- måste ha stöd i dataskyddsförordningen för att få behandla personuppgifter
- bara får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål
- inte ska behandla fler personuppgifter än vad som behövs för ändamålen
- ska se till att personuppgifterna är riktiga
- ska radera personuppgifterna när de inte längre behövs
- ska skydda personuppgifterna, till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs
- ska kunna visa att och hur de lever upp till dataskyddsförordningen.

Enligt dataskyddsförordningen har de registrerade rättigheter som innebär att de har rätt att t ex få information om hur deras personuppgifter behandlas och att de t ex kan få personuppgifter rättade och raderade, om ingen annan lag hindrar.

Kommunens personuppgiftsansvariga, dvs nämnderna, har ansvaret för att dataskyddsförordningen följs. Om dataskyddsförordningen inte följs finns det en risk att enskildas personliga integritet utsätts för risker.

Dataskyddsombudets roll

Dataskyddsförordningen finns, som redan nämnts, för att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Därför finns det ett krav på att vissa organisationer, så som myndigheter, ska ha dataskyddsombud. Dataskyddsombudet utför sitt arbete med de registrerades perspektiv och uppdraget är enligt artikel 39 att ge råd och information till nämnderna och deras organisationer om deras skyldigheter enligt förordningen och att övervaka efterlevnaden samt att vara kontaktpunkt för tillsynsmyndigheten Integritetsskyddsmyndigheten, IMY, och registrerade, dvs de personer vars personuppgifter behandlas i kommunen. Dataskyddsombudet ansvarar inte för att dataskyddslagarna efterlevs i organisationen.

Dataskyddsombudet övervakar efterlevnaden av dataskyddslagarna åt nämnderna och rapporterar till nämnderna, minst en gång per år. Det är i egenskap av min roll som dataskyddsombud som jag har skrivit denna årsrapport med rekommendationer som rör dataskydd.

Kontroller 2023

Dataskyddsförordningen innehåller skyldigheter för de personuppgiftsansvariga. I år har jag valt att titta på vissa grundläggande krav och förutsättningar för att efterleva dataskyddsförordningen. De områden som kontrollen rör är följande:

- Nämndens dataskyddsorganisation
- Registerförteckning
- Personuppgiftsbiträdesavtal
- Personuppgiftsincidenter
- Utbildning i dataskydd för personal
- Konsekvensbedömningar (DPIA)

Resultatet baseras på kontroller som genomfördes under hösten 2023 via frågeformulär och viss dialog. Förändringar kan därför ha skett efter det. Resultatet baseras även på observationer under året.

Nämndens dataskyddsorganisation

Varje nämnd är personuppgiftsansvarig för de personuppgifter som behöver behandlas i deras verksamheter och ansvarar för att dataskyddsförordningen och andra lagar och regelverk som styr behandlingen av personuppgifter efterlevs. Enligt dataskyddsförordningen finns krav på att personuppgiftsansvarig ska ha utsett ett dataskyddsombud. I kommunen finns beslut om att varje nämnd ska ha minst en dataskyddssamordnare som antingen är placerad i den egna förvaltningen eller centralt i Seviceförvaltningen. Nämnden har en skyldighet att kunna hantera det som krävs utifrån dataskyddslagarna. Om roller och ansvarsfördelning i kommunen finns att läsa i Anvisningar för behandling av personuppgifter.

Vårt samhälle och även Eskilstuna kommun står inför de utmaningar som digitalisering innebär bl a vad gäller kompetens för genomförandet. Dataskyddskompetens behövs för stöd vid anskaffning eller utveckling av digitala tjänster och ny teknik men också som stöd i mer vardaglig hantering av personuppgifter.

Resultat

Nämnden har tillgång till stöd av dataskyddsombud och dataskyddssamordnare och uppfyller därmed lagkrav och kommunens styrande dokument. Under året har en hösten 2023 det skett en förbättring i form av utökad dataskyddsorganisation.

Rekommendation

Då det behövs mycket stöd i dataskyddsarbete både för att upprätthålla grunddokumentation, hantera incidenter och i samband med upphandlingar och digitalisering behöver nämnden bevaka detta så att brist på stöd inte blir ett hinder i digitaliseringsarbete och annat dataskyddsarbete, och att man utökar vid behov.

Registerförteckning (Artikel 30)

Personuppgiftsansvariga har en skyldighet att föra ett register över sina personuppgiftsbehandlingar. Registerförteckningen ska upprättas skriftligen, vara tillgänglig i elektroniskt format och hållas uppdaterad. På begäran ska registret göras tillgängligt för IMY.

Innehållet i registerförteckningen har inte granskats under arbetet med kontrollerna då det pågår ett arbete med att komplettera och uppdatera den vilket innebär förändring. Resultatet baseras på input från förvaltningen. Ytterligare utveckling inom området planeras framöver för att underlätta hanteringen av förteckningarna. I viss mån är de även vanligtvis under ständig förändring på så sätt att när nya behandlingar tillkommer eller görs på ett nytt sätt, samt när behandlingar upphör så ska informationen i registerförteckningarna uppdateras.

Resultat

Nämnden har en registerförteckning men det är oklart om den är fullständig. Ett arbete med inventering av personuppgiftsbehandlingar och uppdateringar av registerförteckning planeras. Uppdatering sker även kontinuerligt när nya behandlingar av personuppgifter tillkommer.

Rekommendation

Min rekommendation är inventering och komplettering sker enligt plan så att dokumentationen i registerförteckningen uppfyller minst minimumlagkrav då en komplett registerförteckning är en förutsättning för att ha ordning på sina personuppgiftsbehandlingar och att tillgodose de registrerades rättigheter, t ex när de registrerade begär registerutdrag över sina personuppgifter enligt artikel 15. De fält som minst ska fyllas i enligt dataskyddsförordningen är följande:

- Namn och kontaktuppgifter för den personuppgiftsansvariga, den personuppgiftsansvarigas företrädare samt dataskyddsombudet.
- Ändamålen med behandlingen.
- En beskrivning av kategorierna av registrerade och kategorierna av personuppgifter.
- De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut.
- I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation.
- Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter. Ej enbart hänvisning till informationshanteringsplan utan de faktiska tidsfristerna.
- Om möjligt, en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder.

Dessa fält är obligatoriska och måste vara korrekt ifyllda för att lagkrav ska uppfyllas. Även informationen i de frivilliga fälten ska enligt dataskyddsförordningen finnas dokumenterad någonstans och det är därför en fördel att även fylla i de dessa så att informationen finns samlad.

Samtliga typer av personuppgiftsbehandligar behöver bli identifierade. Utöver de behandlingar som finns i olika IT-system behöver även de behandlingar som förekommer i t ex e-post, system för digitala möten, samarbetsytor, kontorsprogram, appar och sociala medier mm identifieras. Dessa behöver även gås igenom för att se om det finns några som behöver avslutas.

Det finns en mall i kommunen för alla nämnder att använda och en instruktion för hur fälten fylls i.

Personuppgiftsbiträdesavtal (Artikel 28 och 5)

Enligt artikel 28.1 ”ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning och säkerställer att den registrerades rättigheter skyddas.”

För att säkerställa att de behandlar personuppgifter korrekt behövs ett personuppgiftsbiträdesavtal. Personuppgiftsbiträdesavtal behöver skrivas när t ex en leverantör behandlar personuppgifter för nämndens räkning vilket t ex sker när lagring görs på leverantörens servrar när man använder en digital tjänst eller system eller om de på andra sätt behandlar personuppgifter. Det är då nämnden/förvaltningen som bestämmer hur och varför personuppgifterna behandlas.

Biträdet får inte behandla personuppgifterna för egen räkning, t ex i samband med utveckling eller marknadsföring. Om biträdet börjar bestämma över behandlingen kan de bli personuppgiftsansvariga och nämnden och de registrerade förlorar kontrollen över personuppgifterna.

Kommunen använder i regel SKR:s mall och en ny version kom under 2023. Det finns även fall där leverantörens mall används pga att vissa leverantörer använder så kallade standardavtal. Även när standardavtal används ansvarar nämnderna för att de efterlever dataskyddsförordningen.

Resultat

Det saknas i vissa fall personuppgiftsbiträdesavtal med leverantörer som behandlar personuppgifter för nämndens räkning. Hur många som saknas är inte känt.

Rekommendation

Min rekommendation är att de personuppgiftsbehandlingar som saknar personuppgiftsbiträdesavatal identifieras och att det säkerställs att de har giltiga och adekvata personuppgiftsbiträdesavtal med instruktioner till biträdet och lista på underbiträden samt att man har säkerställt att underbiträdena är lämpliga. Detta

behöver göras skyndsamt då avsaknad av personuppgiftsbiträdesavtal är en risk för både de registrerade personerna som omfattas av behandlingen och för nämnden då det inte finns kontroll över hur personuppgifterna behandlas av leverantörerna.

Personuppgiftsincidenter (Artikel 33)

Om personuppgifter inte behandlas på ett korrekt och säkert sätt utsätts registrerade personer för risker som kan få konsekvenser så som att de förlorar kontrollen över sina personuppgifter, kan drabbas av ID-stöld, förlust av konfidentialitet, ekonomisk eller social nackdel mm. Om det inte är osannolikt att en personuppgiftsincident leder till en risk för personen ska incidenten enligt dataskyddsförordningen anmälas till IMY inom 72 timmar från upptäckt. Vid hög risk ska drabbade personer informeras om händelsen.

Exempel på personuppgiftsincidenter kan vara:

- En obehörig får tillgång till personuppgifter, till exempel om någon skickar personuppgifter till en mottagare som inte ska ha dem.
- Datorer eller mobiltelefoner som innehåller personuppgifter förloras eller stjäls.
- Någon ändrar personuppgifter utan tillstånd.
- Personuppgifter är inte längre tillgängliga för den som behöver dem och det leder till negativa konsekvenser för de registrerade, t ex när ett system inte är tillgängligt.

Personuppgiftsincidenter behöver dokumenteras. Det gäller både de som anmäls till IMY och de som inte anmäls. Dokumentationen behöver t ex innehålla en beskrivning av händelsen och vilka som har drabbats, vidtagna och planerade åtgärder, en riskanalys och de beslut som har fattats. När personuppgiftsincidenter rapporteras till IMY sparas den kopia av anmälan som finns att ladda hem efter gjord anmälan i IMY:S digitala tjänst och den utgör en del av dokumentationen. Det finns stöddokument för dokumentation. Det finns ett lagkrav på att dataskyddsombudet involveras.

I en stor organisation är det inte helt lätt att nå ut med information så att alla får kunskap om hur man identifierar en incident. Det har i vinter tagits fram en kort digital utbildning för att underlätta.

Resultat

De incidenter som rapporteras dokumenteras, t ex så ska anmälan till IMY sparas. Vissa brister finns på området t ex vad gäller om alla incidenter dokumenteras korrekt och om vissa delar som behöver dokumenteras finns med. Stöddokument för dokumentation finns och utveckling av dessa är planerade.

Under 2023 har nämnden haft 27 personuppgiftsincidenter, varav 19 har anmälts till IMY.

Incidenter som inte anmäls till IMY förs in i en förteckning.

Dataskyddsombudet rådfrågas och hålls vid behov uppdaterad löpande under arbetet med vissa incidenter. När det gäller mindre incidenter eller incidenter som är repetitiva informeras dataskyddsombudet i vissa fall.

Följande brister när det gäller personuppgiftsincidenter förekommer hos nämnden:

- I nuläget rapporteras troligen inte alla incidenter in från verksamheterna.
- Det förekommer att incidenter rapporteras in sent från verksamheterna.
- Dokumentation är inte komplett och saknar i vissa fall t ex riskanalys eller vissa åtgärder.

Rekommendation

Mina rekommendationer är följande:

- Att information ges till verksamheterna så att incidenter rapporteras in och att de rapporteras in direkt när de händer.
- Att personuppgiftsincidenter dokumenteras enligt krav.

Utbildning i och information om dataskydd för personal

För att personuppgifter ska kunna behandlas på ett korrekt sätt behöver personal utbildas i och/eller informeras om hur det ska ske. Alla behöver ha minst grundläggande kunskaper om behandling av personuppgifter och vissa roller så som specialister inom olika områden behöver fördjupade kunskaper som är relevanta för rollen.

Kommunen har en digital grundutbildning i dataskydd sedan flera år tillbaka som alla medarbetare kan ta del av men som inte är obligatorisk.

Det har i kommunen under vintern tagits fram en kort digital utbildning för medarbetare i att identifiera personuppgiftsincidenter för att förbättra förståelsen och kunskapen om incidenter så att fler incidenter kan identifieras och rapporteras utan dröjsmål. Denna har dock inte hunnit bli tillgänglig för medarbetarna under 2023.

Resultat

Kommunen har en digital grundutbildning i dataskydd sedan flera år tillbaka som alla medarbetare kan ta del av men som inte är obligatorisk.

Alla medarbetare ska ha fått en grundläggande information om GDPR och under perioden 220901 – 230831 har vissa utbildningsinsatser gjorts efter önskemål samt att medarbetare informerats om att det finnsmöjlighet att delta i utbildning.

Rekommendation

Mina rekommendationer är följande:

- Att det blir obligatoriskt för alla att gå en utbildning, t ex en digital utbildning för att öka förståelsen och kompetensnivån allmänt i organisationen. Även de som gick för några år sedan behöver gå igen.

- Att vissa roller får en fördjupad utbildning eller en riktad utbildning för just den funktionen.

Konsekvensbedömningar (DPIA) (Artikel 35)

En konsekvensbedömning behöver göras enligt dataskyddsförordningen i de fall som en behandling av personuppgifter innebär en hög risk för de personer vars personuppgifter ska behandlas, dvs de registrerade. Konsekvensbedömningen kallas även DPIA, Data Protection Impact Assessment.

Den är ett verktyg för att dokumentera, identifiera risker och konsekvenser för personer och ta fram åtgärder för att förebygga riskerna. Man bedömer utifrån vissa fasta kriterier om en konsekvensbedömning ska göras. Den påbörjas tidigt och används under hela projektet, upphandlingsarbetet eller inför en organisationsförändring. Den behöver vara klar innan implementeringen men ska sedan fortsätta att vara ett levande dokument under hela behandlingens livscykel och uppdateras vid behov eller årligen.

Beskrivningen ska vara så tydlig att en utomstående förstår.

Behandlingar som behöver en konsekvensbedömning är t ex när ny teknik eller innovativa lösningar ska genomföras. Det behöver även i regel göras när behandlingen innehåller känsliga eller extra skyddsvärda personuppgifter och rör brukare, klienter, barn eller elever.

Dataskyddsförordningen ställer krav på att dataskyddsombudet rådfrågas i samband med konsekvensbedömningen. Dataskyddsombudets bedömning av lagligheten enligt dataskyddslagarna och rekommendationer bör dokumenteras i konsekvensbedömningsmallen.

Resultat

Arbetet med konsekvensbedömningar går framåt trots att de är tidskrävande och att det är en utmaning att dokumentera tillräckligt, bedöma risker och ta fram åtgärder. De görs inte alltid när det finns krav utan prioriteringar har gjorts utifrån resurser då de är tidskrävande.

Under perioden 220101 – 230831 har 7 konsekvensbedömningar gjorts antingen slutförts eller påbörjats.

Dataskyddsombudet rådfrågas oftast inför konsekvensbedömningar och ombeds att granska och bedöma laglighet när konsekvensbedömningen bedöms vara klar.

Det finns vissa brister:

- Det saknas vissa konsekvensbedömningar.
- Dokumentationen är i vissa fall något knapphändig.
- Det finns fall där dataskyddsombudets råd inte har följts. Motivering har dock dokumenterats.

Rekommendation

Mina rekommendationer är att nämnden:

- Utför de konsekvensbedömningar som saknas.
- Säkerställer att beskrivningarna är tillräckligt tydliga så att en utomstående förstår behandlingen och hur den kommer att hanteras.

Dataskyddsombudets arbete i kommunen under 2023

Under 2023 har arbetet bestått av bl a följande:

- Rapporterat om dataskyddet till nämnder och förvaltningschefer för 2022.
- Stöd i frågor om dataskydd i korta så väl som mer tidskrävande ärenden.
- Givit råd och övervakat vid dataskyddsarbete på kommunövergripande nivå och nämndnivå. T ex i upphandlingar och projekt, samt vid framtagande av styrande dokument.
- Varit rådgivande i arbetet med processer.
- Skrivit olika informationsdokument om behandling av personuppgifter utifrån dataskyddsförordningen.
- Skrivit nyhetsbrev.
- Informerat om dataskydd.
- Omvärldsbevakat och förmedlat omvärldsbevakning till berörda i kommunen.
- Övervakat behandling av personuppgifter.
- Utfört kontroller.
- Svarat på frågor från registrerade.
- Hållit sig uppdaterad inom dataskyddsområdet genom att delta i utbildningar, webbinarier och konferenser.
- Sammankallat till nätverksmöten med övriga i kommunens dataskyddsorganisation.
- Deltagit i nätverksmöten för dataskyddsombud.

Dataskyddsombudets årsrapport till nämnden för 2023 avseende dataskydd

Denna rapport är en årsrapport för dataskydd hos nämnden för 2023. Innehållet är avgränsat och inte en fullständig rapport över nämndens dataskydd under året. Resultatet av höstens kontroll ger en ögonblicksbild och därför kan förändringar ha skett efter kontrollen.

EU:s dataskyddsförordning (GDPR) gäller som lag i samtliga EU-länder, inklusive Sverige. Den har sina rötter i Europakonventionen om de mänskliga rättigheterna och finns till för att skydda enskildas (de registrerades) grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Varje behandling av personuppgifter behöver uppfylla dataskyddsförordningen och dess grundläggande principer.

Det finns krav i förordningen att vissa typer av organisationer, så som kommuner ska ha ett dataskyddsombud som är en oberoende roll med uppdraget att ge råd och informera utifrån dataskyddsförordningen och övervaka att organisationen följer den.

Som dataskyddsombud rapporterar jag till samtliga 14 nämnder om dataskyddet och uppfyllandet av dataskyddsförordningen samt övriga bestämmelser som gäller skyddet av personuppgifter.

Kommunens personuppgiftsansvariga, dvs nämnderna, har ansvaret för att dataskyddsförordningen följs.

När personuppgiftsansvariga inte kommer att följa rekommendationerna bör en motivering dokumenteras.

Svar till dataskyddsombudet bör lämnas.

Med vänlig hälsning

Charlotte Nilsson
Dataskyddsombud