



Nulägesanalys

Efterlevnad av dataskyddsförordningen

Kommunstyrelsen

2025

Nulägesanalys

Efterlevnad av dataskyddsförordningen Kommunstyrelsen

Beatrice Helmersson

© Beatrice Helmersson och Huddinge kommun

Tryckeri, 2025

ISBN 91-85565-02-4

Innehåll

Rapport avseende resultat av nulägesanalys – efterlevnad av	
dataskyddsförordningen.....	4
Inledning	4
Syfte	4
Metod	4
Sammanfattning	4
Resultat.....	6
Grundläggande principer och rättslig grund.....	6
Registrerades rättigheter.....	8
Personuppgiftsbehandlingar	9
Personuppgiftsbiträden och överföring.....	10
Säkerhet och incidenthantering	11
Organisation	13

Rapport avseende resultat av nulägesanalys – efterlevnad av dataskyddsförordningen

Inledning

Dataskyddsombudet har utfört en nulägesanalys med fokus på kommunstyrelsens behandling av personuppgifter och hur väl man efterlever dataskyddsförordningens krav. Utförandet av nulägesanalysen har även varit ett bra sätt att lära känna verksamheterna och få ett grepp om vilka personuppgifter som behandlas i olika flöden. Resultatet av nulägesanalysen kan komma att ligga till grund för dataskyddsombudets kommande tillsyn av kommunstyrelsens verksamhetsområde.

Syfte

Syftet med nulägesanalysen är att skapa en övergripande och samlad bild av kommunstyrelsens arbete med dataskydd och graden av efterlevnad av dataskyddsförordningens krav. Vid identifierade brister redovisas förslag till åtgärder för att stärka efterlevnaden och minska riskerna för eventuella sanktioner vid tillsyn.

Metod

Syftet med nulägesanalysen är att skapa en övergripande och samlad bild av kommunstyrelsens arbete med dataskydd och graden av efterlevnad av dataskyddsförordningens krav. Vid identifierade brister redovisas förslag till åtgärder för att stärka efterlevnaden och minska riskerna för eventuella sanktioner vid tillsyn.

Sammanfattning

Nedan följer en sammanfattande redogörelse av de positiva aspekterna samt de brister som resultatet visar. För en detaljerad redogörelse hänvisas till efterföljande kapitel.

Sammanfattningsvis kan de positiva aspekterna sammanfattas enligt följande.

- Det finns en tydlig vilja att göra rätt och ett intresse för informationssäkerhet, dataskydd och integritetsfrågor inom kommunstyrelsens verksamhetsområden.
- Ledningen uppvisar en tydlig ambition att efterleva dataskyddsförordningen med ökade resurser i form av ny tillsatt dataskyddssamordnarfunktion.
- Det finns en grundstruktur genom exempelvis GDPR-handbok och Riktlinjer för hantering av personuppgifter att utgå ifrån i det fortsatta arbetet. Dessa behöver förvisso utvecklas, men det finns en grund att utgå ifrån.

Sammanfattningsvis kan de brister som uppdragets sammanfattas enligt följande.

- Det saknas ett komplett behandlingsregister för kommunstyrelsens personuppgiftsbehandlingar. Att ha ett uppdaterat behandlingsregistret på plats i organisationen är en central del i dataskyddsarbetet i sin helhet med tanke på bland annat ansvarsprincipen, hantering av rättighetsbegäranden samt för att kunna säkerställa att personuppgiftsbehandlingar faktiskt är lagliga.
- Det framgår inte tydligt att det ges korrekt och uttömmande information till de registrerade i samband med att personuppgifter samlas in. Det finns viss information på webben (huddinge.se) samt viss information i anställningsavtalet. Dock är denna information inte förenligt med kraven i artiklarna 12-14.
- Det saknas en tydlig verksamhetsförankrad struktur kopplat till styrdokument på området (exempelvis GDPR-handboken), som redogör för vilka åtgärder som bör vidtas inför att en personuppgiftsbehandling ska påbörjas, medan den pågår samt när den ska avslutas. Genom att inte ha detta på plats finns risk för att de grundläggande principerna för behandling åsidosätts samt att personuppgiftsbehandlingen kan grundas på en inkorrekt rättslig grund.

Sammantaget är dataskyddsombudets bedömning att efterlevnadsnivån är låg till måttlig (på en skala mycket låg, låg, måttlig, hög).

Utifrån resultatet rekommenderar dataskyddsombudet att samtliga åtgärder vidtas för att öka efterlevnaden av dataskyddsförordningen samt för att minska riskerna för de registrerade samt i förlängningen för sanktioner vid tillsyn.

Dataskyddsombudet har nedan sammanfattat de fem mest prioriterade åtgärderna för förvaltningen att arbeta vidare med.

1. Inventera vilka personuppgiftsbehandlingar som utförs inom den personuppgiftsansvariges verksamhet och kartlägg dessa i behandlingsregistret.
2. Säkerställ att de registrerade får information om hur personuppgifter kommer att behandlas, enligt artiklarna 12-14 i dataskyddsförordningen, innan dess att personuppgiftsbehandlingen påbörjas.
3. Säkerställ att informations-/dokumenthanteringsplanerna är kompletta inom samtliga områden, är väl kända inom förvaltningen samt att det är tydligt vilken funktion som ska gallra uppgifter och när det ska ske.
4. Uppdatera GDPR-handboken och upprätta sedan checklistor utifrån GDPR-handboken som tydliggör vilka åtgärder som ska vidtas inför en personuppgiftsbehandling påbörjas, under pågående personuppgiftsbehandling samt vid avslut av personuppgiftsbehandling. Såsom exempelvis, ej begränsat till, konsekvensbedömning, inbyggd dataskydd och dataskydd som standard, registrering av personuppgiftsbehandling i behandlingsregister och så vidare.
5. Genomför utbildningsinsatser för personal, såväl generellt om informationssäkerhet och dataskydd som specifikt inom olika områden såsom exempelvis, ej begränsat till, konsekvensbedömning, incidenthantering och registrerades rättigheter.

Resultat

I detta kapitel presenteras resultatet av nulägesanalysen. Resultatet presenteras utifrån respektive kontrollområde och varje kontrollområde är i sin tur kopplat till ett eller flera krav i dataskyddsförordningen. Samtliga kontrollområden presenteras med en förklaring av kravet samt bedömning av kontrollområdets uppfyllelse. Ett kontrollområde kan bedömas som "uppfyllt", "delvis uppfyllt" eller "inte uppfyllt". Observera att ett kontrollområde kan klassificeras som "delvis uppfyllt", trots att det till stor del kan anses uppfyllt. Det är ofta en bedömning där flera aspekter vägs in. Dataskyddsombudets rekommendationer redogörs för i bilagorna "sammanfattande åtgärdsplan" och "detaljerad åtgärdsplan".

Grundläggande principer och rättslig grund

De grundläggande principerna för personuppgiftsbehandling utgör kärnan i dataskyddsförordningen och återfinns i artikel 5. Principerna omfattar bland annat laglighet, korrekthet, ändamålsbegränsning, uppgiftsminimering och lagringsminimering. Varje behandling av personuppgifter måste dessutom vila på en giltig rättslig grund enligt artikel 6. Att dessa principer följs och dokumenteras är avgörande för laglig och transparent behandling av personuppgifter inom kommunstyrelsens verksamhet.

Uppfylls kontrollområdet?

Delvis uppfyllt

Kommentarer

De grundläggande principerna för behandling av personuppgifter, såsom lagringsminimering, uppgiftsminimering och ändamålsbegränsning, beskrivs i Huddinge kommuns *Riktlinjer för behandling av personuppgifter (HKF 1500)* samt i *Dataskyddsombudets rekommendationer för GDPR-handbok med huvudsakliga dataskyddsregler för Huddinge kommuns medarbetare*. Dokumenten ger en övergripande beskrivning av principernas innebörd men saknar mer konkreta anvisningar för hur de ska tillämpas i praktiken, vilket leder till otydlighet i det dagliga arbetet med dataskydd.

När det gäller principen om lagringsminimering finns det informations- och dokumenthanteringsplaner för kommunstyrelseförvaltningens olika avdelningar, i vissa fall även på sektionsnivå. Dessa planer är dock inte enhetligt uppdaterade; flera upprättades redan 2018 och har inte reviderats sedan dess, medan någon plan har uppdaterats 2021/22. I intervjuer framkommer att uppfattningarna skiljer sig åt kring planernas aktualitet och tydlighet. Vissa menar att det finns tillräckliga rutiner och ansvarsfördelning, medan andra upplever att det är oklart vem som ansvarar för gallring, när den ska ske och hur den ska genomföras. Det framkommer även att e-post i funktionsbrevlådor och filer i gemensamma mappar ofta sparas längre än nödvändigt, och att det ibland förekommer sekretessbelagda uppgifter i dessa mappar utan att tillgången är behörighetsstyrd. I samband med upphandling av nya system ställs vanligen krav på att automatisk gallring ska vara möjlig, men det finns fortfarande system där gallring inte kan utföras eller där behovet av gallring inte är tydligt utrett.

Principen om uppgiftsminimering beskrivs övergripande i HKF 1500 men utan vägledning för hur den ska säkerställas i praktiken. En allmän förståelse för principens innebörd finns, men flera intervjuade upplever svårigheter i tillämpningen. Det finns risk för att onödiga personuppgifter samlas in, exempelvis genom listor och e-postkorrespondens, samt brister i dokumentationen av bedömningar av vilka uppgifter som är nödvändiga. Systemsäkerhetsanalyser (SSA) genomförs ofta inför upphandling av nya system, vilket bidrar till att begränsa insamlingen av onödiga uppgifter. SSA-mallen innehåller frågor om vilka personuppgifter som ska behandlas och om de är känsliga, vilket kan skapa medvetenhet kring behovet. Samtidigt finns en risk att pågående behandlingar som inte omfattas av upphandling inte granskas med avseende på proportionalitet och nödvändighet, vilket kan leda till att uppgiftsminimeringsprincipen inte beaktas fullt ut.

Även principen om ändamålsbegränsning är beskriven i HKF 1500 och i GDPR-handboken. Den personuppgiftsansvarige får endast samla in och behandla personuppgifter som är relevanta och nödvändiga för ett specifikt ändamål, och behandlingen får endast ske enligt de ändamål som anges i nämndernas behandlingsregister. Granskning visar dock att dessa register inte alltid är uppdaterade eller fullständiga, vilket innebär risk för ändamålsglidning. Det är inte heller tydligt hur principen tillämpas i det dagliga arbetet, och få av de intervjuade kan beskriva hur ändamålsbegränsning säkerställs i praktiken.

Granskningen visar även brister i beskrivningen av rättslig grund för flera personuppgiftsbehandlingar. I vissa fall anges rättsliga grunder som inte överensstämmer med dataskyddsförordningen, och i andra fall saknas helt uppgift om rättslig grund. Majoriteten av behandlingarna tycks baseras på myndighetsutövning, vilket är vanligt inom kommunal verksamhet, men även andra grunder såsom uppgift av allmänt intresse eller rättslig förpliktelse kan vara aktuella. Det finns därför ett behov av att tydliggöra vilka rättsliga grunder som är tillämpliga i olika situationer och vad dessa innebär.

Vidare har dataskyddsombudet identifierat att samtycke i vissa fall används som rättslig grund på ett sätt som inte är förenligt med dataskyddsförordningen, till exempel vid rekrytering där beroendeförhållandet mellan arbetssökande och arbetsgivare gör samtycke olämpligt. Även vid behandling av bilder finns brister, framför allt gällande tydlig information om hur samtycke kan återkallas. Den e-tjänst som används för att lämna och återkalla samtycke till bildpublicering fungerar som ett viktigt verktyg, men det framgår inte tydligt hur ordning och dokumentation av samtycken säkerställs i praktiken.

Slutligen framgår att ansvarsskyldigheten enligt dataskyddsförordningen inte fullt ut är uppfylld. Det saknas uppdaterade behandlingsregister, tydliga styrdokument och utbildningar för personalen. Konsekvensbedömningar genomförs inte systematiskt och dokumentation av beslut och analyser kopplade till dataskydd är bristfällig. Sammantaget visar granskningen på ett behov av stärkt intern styrning, tydligare ansvarsfördelning och ökad medvetenhet om hur de grundläggande principerna för behandling av personuppgifter ska tillämpas och dokumenteras i praktiken.

Registrerades rättigheter

De registrerades rättigheter regleras i artiklarna 12–23 i dataskyddsförordningen och syftar till att ge enskilda kontroll över sina personuppgifter. Det omfattar bland annat rätt till information, tillgång, rättelse, radering, begränsning av behandling, invändning samt dataportabilitet. För att kommunen ska kunna uppfylla sina skyldigheter krävs tydliga rutiner, information till de registrerade och en effektiv hantering av inkomna begäranden.

Uppfylls kontrollområdet?

Inte uppfyllt

Kommentarer

Utifrån de uppgifter som framkommit vid intervjuerna bedöms kännedomen om de registrerades rättigheter som relativt god. Det finns information på intranätet som beskriver vilka rättigheter som gäller enligt dataskyddsförordningen och som ger en kortfattad förklaring till vissa av dem. Mer detaljerad information återfinns i GDPR-handboken, där hänvisning görs till en särskild ”Riktlinje om de registrerades rättigheter”. Denna riktlinje verkar dock ännu inte vara upprättad, då den inte går att finna, vilket innebär att det i nuläget saknas praktisk vägledning för hur verksamheten ska tillgodose de registrerades rättigheter.

Av intervjuerna framgår att det råder delade meningar om hur rättighetsbegäranden ska hanteras i praktiken. En gemensam nämnare är att tydliga rutiner och ansvarsbeskrivningar saknas, oavsett vilken rättighet den registrerade önskar utöva. Dataskyddsombudet har inte heller funnit någon formell rutin för hantering av rättighetsbegäranden. Under hösten har den personuppgiftsansvarige mottagit flera sådana begäranden, främst rörande rätten till tillgång, men även rätten till radering och begränsning. Dessa har hanterats utan stöd av dokumenterade rutiner, vilket innebär att kvaliteten och enhetligheten i svaren inte kan säkerställas. Avsaknaden av rutiner, uppdaterade behandlingsregister och tillräcklig kunskap har påverkat hanteringen, även om de inblandade visat en tydlig vilja att göra rätt och samarbeta för att lösa uppgifterna – något som bedöms som mycket positivt.

Vidare framkommer det att de flesta medarbetare inte har närmare kännedom om hur den personuppgiftsansvarige behandlar deras egna personuppgifter i egenskap av anställda. Det finns en skrivelse i anställningsavtalen som berör personuppgiftsbehandling, men den är mycket kortfattad och uppfattas inte som informativ. Skrivelsen lyder:

”Som arbetsgivare får Huddinge kommun lagligt behandla personuppgifter om anställda och uppdragstagare i den utsträckning det är nödvändigt för att fullgöra anställnings- eller uppdragsavtalet.”

Dataskyddsombudet har fått information om att HR-avdelningen påbörjat ett utvecklingsarbete för att revidera anställningsavtalen och förtydliga hur anställdas personuppgifter behandlas, vilket är ett steg i rätt riktning.

På den personuppgiftsansvariges webbplats, huddinge.se, finns en sida som informerar om behandling av personuppgifter enligt GDPR. Denna sida ger dock inte en heltäckande beskrivning och uppfyller inte samtliga krav som anges i

artiklarna 12–14 i dataskyddsförordningen. Dataskyddsombudet har även granskat ett urval av den personuppgiftsansvariges e-tjänster och konstaterat att ingen av dessa innehåller fullständig information om hur personuppgifter behandlas, sett till de krav som ställs. Enligt dataskyddsförordningen ska registrerade få klar och tydlig information om hur deras personuppgifter behandlas i en specifik behandling, och detta ska ske innan behandlingen påbörjas. Denna skyldighet uppfylls inte fullt ut i dagsläget, även om det kan finnas e-tjänster utanför granskningen där sådan information anges.

Sammantaget visar granskningen att det finns en grundläggande förståelse för de registrerades rättigheter, men att verksamheten saknar tydliga rutiner, styrdokument och praktisk vägledning för att säkerställa att dessa rättigheter tillgodoses på ett enhetligt och rättssäkert sätt.

Personuppgiftsbehandlingar

Varje personuppgiftsbehandling ska dokumenteras och kunna redovisas enligt artikel 30 i dataskyddsförordningen. Detta innebär att den personuppgiftsansvarige ska föra ett aktuellt och fullständigt register över de personuppgiftsbehandlingar som utförs, inklusive uppgifter om ändamål, rättslig grund, gallringsfrister och mottagare.

Dessutom ska konsekvensbedömningar enligt artikel 35 genomföras när en behandling sannolikt medför hög risk för fysiska personers rättigheter och friheter. Ett uppdaterat behandlingsregister och strukturerad hantering av konsekvensbedömningar är centralt för den personuppgiftsansvariges/kommunstyrelsens regelefterlevnad.

Uppfylls kontrollområdet?

Inte uppfyllt

Kommentarer

Dataskyddsombudet har konstaterat att det finns tre behandlingsregister kopplade till den personuppgiftsansvarige. Samtliga register är senast uppdaterade 2018. Två av registren omfattar behandlingar inom HR medan det tredje innehåller uppgifter om behandlingar från flera avdelningar. Det är dock oklart om alla pågående personuppgiftsbehandlingar finns redovisade i dessa register samt vilket av registren som i nuläget är det mest aktuella.

Under intervjuerna framkommer att ingen av de intervjuade har varit delaktig i arbetet med behandlingsregistren. Det råder även osäkerhet kring vad ett behandlingsregister är, vilken funktion som ansvarar för dess uppdatering och vilket ansvar den personuppgiftsansvarige har för att säkerställa att registret hålls aktuellt.

Det framgår vidare att en systemsäkerhetsanalys (SSA) vanligtvis genomförs innan upphandling av nya IT-system påbörjas. Enligt GDPR-handboken och den information som finns på intranätet ska SSA alltid genomföras inför upphandling och det är objektägarens ansvar att säkerställa att samtliga system inom ansvarsområdet har genomgått en sådan analys. I SSA-mallen finns en särskild del

som berör personuppgiftsbehandling. Den innehåller uppgifter om ändamål med behandlingen, kategorier av registrerade och personuppgifter som behandlas, förekomst av känsliga personuppgifter, mottagare av uppgifterna, vidtagna säkerhetsåtgärder samt eventuell överföring till tredjeland.

Att genomföra en SSA inför inköp av nya system är positivt ur ett dataskyddsperspektiv eftersom viktiga aspekter då beaktas redan i planeringsskedet. Samtidigt är en SSA inte detsamma som en konsekvensbedömning avseende dataskydd. Centrala delar som fastställande av rättslig grund, bedömning av de grundläggande principerna för behandling och uppdatering av behandlingsregistret ingår inte i SSA-processen.

Intervjuerna visar att det råder oklarhet kring när en konsekvensbedömning avseende dataskydd ska genomföras. Det finns även en risk att mindre omfattande behandlingar, eller behandlingar som inte är kopplade till upphandling av nya system, förbises. Flera av de intervjuade uttrycker behov av ytterligare stöd vid genomförandet av konsekvensbedömningar och vid bedömning av lämpliga skyddsåtgärder.

Vidare framgår att konsekvensbedömningar ofta uppfattas som en engångsåtgärd som genomförs inför ett projekt eller ett systeminförande. Enligt dataskyddsombudet bör konsekvensbedömningar i stället ses som en pågående process som kontinuerligt följs upp och revideras utifrån förändringar i verksamheten, nya risker eller uppdaterade behandlingar.

Sammantaget visar granskningen att den personuppgiftsansvarige behöver säkerställa att behandlingsregistren hålls aktuella, att ansvarsfördelningen tydliggörs och att rutiner för konsekvensbedömningar etableras och tillämpas löpande. Detta är centralt för att kunna uppfylla dataskyddsförordningens krav på ansvarsskyldighet och säkerställa en rättssäker hantering av personuppgifter.

Personuppgiftsbiträden och överföring

När den personuppgiftsansvarige anlitar externa leverantörer som behandlar personuppgifter å dess vägnar betraktas dessa som personuppgiftsbiträden enligt artikel 28 i dataskyddsförordningen. Den personuppgiftsansvarige måste säkerställa att biträdena ger tillräckliga garantier för att genomföra lämpliga tekniska och organisatoriska säkerhetsåtgärder.

Vidare reglerar artiklarna 44–50 överföring av personuppgifter till tredje land (länder utanför EU/EES). Dessa överföringar får endast ske under förutsättning att en adekvat skyddsnivå säkerställs, exempelvis genom standardavtalsklausuler eller beslut om adekvat skydd.

Uppfylls kontrollområdet?

Uppfylls

Kommentarer

Av intervjuerna framgår att begreppet personuppgiftsbiträde är välkänt och att det i stor utsträckning finns personuppgiftsbiträdesavtal tecknade med leverantörer

som behandlar personuppgifter för den personuppgiftsansvariges räkning. Däremot har ingen uppföljning eller granskning av dessa biträden genomförts för att säkerställa efterlevnaden av avtalen, vilket innebär en brist i kontrollen över hur personuppgifter hanteras av externa parter.

Det framgår inte heller att den personuppgiftsansvarige ingår i några gemensamma personuppgiftsbehandlingsåtgärder tillsammans med andra aktörer. Trots detta rekommenderas att en genomgång görs av befintliga behandlingsåtgärder för att identifiera eventuella behandlingsåtgärder där gemensamt personuppgiftsansvar föreligger och tydliggöra hur dessa ska regleras. Om gemensam behandling förekommer ska detta dokumenteras i en överenskommelse som klargör respektive parts ansvar för att uppfylla skyldigheterna enligt dataskyddsförordningen. Även gemensamma behandlingsåtgärder internt, exempelvis mellan nämnder och styrelse, bör ses över och säkerställas genom gällande reglementen.

Vidare framkommer att den personuppgiftsansvarige använder ett antal IT-tjänster och system där överföring av personuppgifter till tredjeland sker eller kan komma att ske. I samband med upphandling av nya system ställs som grundläggande krav att behandling av personuppgifter ska ske inom EU/EES. Detta krav infördes genom ett beslut som fattades 2022 med anledning av de dataskyddsrisker som identifierats vid användning av amerikanska molntjänster. Beslutet innebär att sådana tjänster endast får användas restriktivt och när det finns välmotiverade skäl. Sedan dess har förutsättningarna förändrats, bland annat genom EU-kommissionens beslut om adekvat skyddsnivå för organisationer anslutna till Data Privacy Framework. Det är därför viktigt att den personuppgiftsansvarige kontinuerligt följer utvecklingen på området och uppdaterar sina bedömningar och riktlinjer i takt med rättsläget.

Det framkommer även att arbete har pågått med att ta fram så kallade exitplaner för att säkerställa att det finns rutiner och handlingsplaner vid behov av att avsluta samarbete med leverantörer eller flytta data från ett system till ett annat.

Dataskyddsombudet har dock inte funnit någon dokumentation som visar att konsekvensbedömningar av dataöverföringar, så kallade *Transfer Impact Assessments* (TIA), har genomförts. En sådan analys är central för att kunna bedöma om en överföring till tredjeland kan ske på ett lagligt sätt och för att säkerställa att nödvändiga skyddsåtgärder införlivas.

Slutligen är det viktigt att beakta att tredjelandsöverföringar inte enbart avser överföringar till USA. Vid upphandling och användning av IT-tjänster bör den personuppgiftsansvarige ta hänsyn till samtliga länder utanför EU/EES och göra motsvarande bedömningar av rättsligt skydd och risker.

Säkerhet och incidenthantering

Enligt artikel 32 i dataskyddsförordningen ska den personuppgiftsansvarige tillförsäkra att personuppgifterna skyddas på ett adekvat sätt. Det ska göras genom att den personuppgiftsansvarige vidtar lämpliga tekniska och organisatoriska

säkerhetsåtgärder - som står i proportion till risken för fysiska personers fri- och rättigheter.

En personuppgiftsincidenter är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter. Den kan också leda till obehörigt röjande eller obehörig åtkomst till personuppgifter. Enligt artiklarna 33-34 i dataskyddsförordningen har den personuppgiftsansvarige ett krav att dokumentera samtliga incidenter som inträffar samt i vissa fall anmäla incidenter till tillsynsmyndigheten och informera registrerade om det inträffade.

Uppfylls kontrollområdet?

Delvis uppfyllt

Kommentarer

Av intervjuerna framgår att den personuppgiftsansvarige vidtar flera olika säkerhetsåtgärder för att skydda personuppgifter på ett adekvat sätt. Bland annat används säker inloggning med BankID, behörighetsstyrning tillämpas och regelbundna säkerhetskopieringar genomförs. Inför varje inköp av IT-system genomförs en systemsäkerhetsanalys (SSA) och i vissa fall även en konsekvensbedömning. Dessa processer syftar bland annat till att identifiera och införa lämpliga säkerhetsåtgärder för att skydda information och personuppgifter.

Trots detta framgår att det finns system som saknar funktioner för loggkontroll och att vissa mappar, innehållande sekretessbelagda, skyddsvärda och känsliga personuppgifter, saknar behörighetsbegränsningar. Det innebär en risk för att obehöriga kan få tillgång till uppgifter som kräver särskilt skydd.

Flera intervjupersoner uppger att det är svårt att avgöra vilken säkerhetsnivå som är tillräcklig för olika typer av personuppgiftsbehandlings. Det upplevs även oklart hur vissa IT-system ska användas på ett säkert sätt, särskilt när hantering av sekretessbelagda eller känsliga uppgifter sker utanför verksamhetssystemen.

När det gäller hantering av personuppgiftsincidenter framkommer en splittrad bild. Vissa upplever att de har god kännedom om hur incidenter ska hanteras, medan andra saknar kunskap inom området. De flesta känner till att vissa incidenter ska anmälas till Integritetsskyddsmyndigheten inom 72 timmar, men det finns ingen tydlig kännedom om hur rapportering ska ske internt.

Viss information om incidenthantering finns på intranätet och i GDPR-handboken. I handboken anges att det ska finnas en process för hantering av personuppgiftsincidenter, men dataskyddsombudet har inte funnit någon dokumenterad process. Varken intranätet eller handboken beskriver konkret hur incidenter ska rapporteras och hanteras i praktiken.

Det finns ett verksamhetssystem, Artwise, som används för att rapportera personuppgiftsincidenter internt. Ingen av de intervjuade verkar dock känna till systemet eller hur rapportering ska ske via detta. Det är även oklart för dataskyddsombudet i vilken omfattning systemet används, vilket bör klargöras.

Sammantaget visar granskningen att det finns ett grundläggande säkerhetsarbete med flera tekniska och organisatoriska skyddsåtgärder, men att rutiner för intern incidentrapportering och loggkontroll behöver förtydligas och kompletteras för att säkerställa en effektiv och rättssäker hantering av personuppgiftsincidenter.

Organisation

Vissa organisationer är skyldiga att utnämna ett dataskyddsombud, bland annat är myndigheter och offentliga organ skyldiga att göra det. Den personuppgiftsansvarige har ett ansvar att säkerställa att dataskyddsombudet får tillräckliga resurser för att kunna utföra sitt arbete och att dataskyddsombudet på ett korrekt sätt och i god tid får delta i alla frågor som rör skyddet av personuppgifter. Dataskyddsombudet ska även samarbeta med tillsynsmyndighet. Kraven rörande dataskyddsombud finns i artiklarna 37-39 i dataskyddsförordningen.

Ett fungerande dataskyddsarbete förutsätter en tydlig ansvarsfördelning och kännedom om rollerna inom organisationen. Ett strukturerat organisatoriskt stöd, i form av dataskyddssamordnare eller liknande funktioner, stärker den operativa efterlevnaden och säkerställer att arbetet är långsiktigt hållbart.

Uppfylls kontrollområdet?

Delvis uppfyllt

Kommentarer

Den personuppgiftsansvarige har utsett ett dataskyddsombud, vilket även har anmälts till Integritetsskyddsmyndigheten. Under hösten har dessutom en dataskyddssamordnare anställts för att stödja dataskyddsarbetet inom organisationen.

Av intervjuerna framgår dock att det råder oklarheter kring vem som innehar rollerna som dataskyddsombud respektive dataskyddssamordnare. Det finns ett tydligt behov av att klargöra roller, kommunikationsvägar och ansvarsområden för dessa funktioner.

Vidare framgår att ansvaret för dataskyddsfrågor i stort är otydligt för många medarbetare. Även om begreppet *personuppgiftsansvarig* är välkänt, är det inte klart hur ansvaret konkret fördelas i praktiken. Det saknas tydlighet kring vilka roller eller funktioner som ansvarar för olika delar av dataskyddsarbetet, exempelvis hantering av register, konsekvensbedömningar och uppföljning av personuppgiftsbiträden.

Det finns därmed ett behov av att stärka den organisatoriska strukturen för dataskydd genom tydlig ansvarsfördelning, bättre intern kommunikation och klargjorda rutiner för samordning mellan dataskyddsombud, dataskyddssamordnare och verksamhetens olika delar.