Göteborgs Stad

Årsrapport för dataskyddsarbetet 2024

Nämnden för Intraservice

2025-02-28

Innehåll

1 Dataskydd i kommunal verksamhet

Dataskyddsförordningen (GDPR) har tillkommit för att särskilt värna om den enskildes rätt till integritet och kontroll över vad som sker med ens personuppgifter. Rätten till en fredad privat sfär och personlig integritet är grundläggande i ett demokratiskt samhälle och är ett av fundamenten på vilket många andra av våra demokratiska rättigheter vilar. Lagstiftningen finns till för att skydda individen från skada och sätter ramarna för hur personuppgifter får behandlas i en alltmer digital värld.

Att förvaltningar och bolag hanterar personuppgifter i enlighet med gällande lag bör vara en självklarhet i syfte att visa omsorg om det förtroende som getts den som har att hantera personuppgifter. För att säkerställa följsamhet gentemot GDPR behöver dataskyddsperspektivet genomsyra arbetet inom de kommunala verksamheterna på alla olika plan. Det gäller allt från rutiner och processer för det dagliga arbetet, till arbetet med innovations- och digitaliseringslösningar för framtidens arbetssätt på förvaltningar och bolag inom Göteborgs Stad. I det framåtsyftande arbetet är GDPR ett viktigt redskap för att kunna säkerställa en digitalisering som håller över tid.

2 Göteborgs Stads dataskyddsombud

Det är varje nämnd och bolag som är ytterst ansvarig för att dess verksamhet följer dataskyddslagstiftningen. För att stödja stadens nämnder och bolag i arbetet med dataskydd har ett dataskyddsombud utsetts. I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud åt stadens bolag och nämnder. Vad som är dataskyddsombudets uppgifter framgår direkt av lagstiftningen i GDPR.[1] Dataskyddsombudets viktigaste uppgift är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. Detta sker bland annat genom att samla in information om hur personuppgifter behandlas och genom att kontrollera hur bestämmelser och interna styrdokument som styr dataskyddsarbetet efterlevs. Dataskyddsombudet har också till uppgift att ge råd och information till förvaltningar och bolag i dataskyddsfrågor. Detta sker genom att dataskyddsombudet är behjälplig när frågor rörande behandlingen av personuppgifter uppkommer hos verksamheterna.

Enligt lag ska dataskyddsombudet även rapportera om arbetet till högsta förvaltningsnivå[2], och utifrån detta lämnar dataskyddsombudet årligen en rapport om den egna verksamhetens dataskyddsarbete till nämnder och bolag i Göteborgs Stad. I rapporten redogör dataskyddsombudet för de iakttagelser som gjorts under året, både stadenövergripande och, i vissa fall, verksamhetsspecifika. Rapporten innehåller även information om årets fördjupade kontroll samt resultatet från den uppföljning som genomförts avseende hur verksamheten hanterat och arbetat med de rekommendationer som lämnades i årsrapporten 2023.

Årsrapporten är avsedd att kunna användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Det är upp till varje verksamhet att besluta om hur det interna dataskyddsarbetet ska utformas utifrån verksamhetens förutsättningar för att på bästa sätt hantera identifierade risker.

2.1 Stadenövergripande iakttagelser 2024

2.1.1 Ny central funktion för styrning och samordning i dataskyddsfrågor möjliggör ett stärkt dataskydd

Hur långt förvaltningar och bolag kommit i dess dataskyddsarbete skiljer sig stort åt inom Staden. Skillnaderna bedöms till stor del bero på bristande styrning och samordning i dataskyddsfrågor från centralt håll, något som lyfts av dataskydds-ombudet under flera år. Resultatet av detta är bland annat att skyddet för de registrerades personuppgifter varierar mellan verksamheterna, en ineffektiv

[1] Artikel 39 i GDPR
[2] Artikel 38.3 i GDPR

personuppgiftsincidenthantering och att hanteringen av rättigheter hanteras olika beroende på vilken verksamhet man vänder sig till.

Dataskyddsombudets förhoppning är att den nya dataskyddsfunktionen som införts på stadsledningskontoret ska bidra till att utveckla och stärka de grundläggande delarna av dataskyddsarbetet och därigenom generera ett mer enhetligt dataskydd inom Staden. Att stadsledningskontoret nu tar ansvar för att samordna dataskyddsarbetet bedöms ligga i linje med kommunstyrelsens uppdrag.

I sammanhanget vill dataskyddsombudet samtidigt poängtera att varje nämnd och bolag fortfarande är ytterst ansvariga för sina respektive personuppgifts-behandlingar. Det är därför även fortsatt upp till varje nämnd och bolag att säkerställa efterlevnad gentemot lagstiftningen. Att varje verksamhet tar det ansvaret är avgörande för att det arbete som görs inom dataskyddsfunktionen ska få genomslag och ha en positiv påverkan på dataskyddet som helhet i Staden.

2.1.2 Verksamhetens ledning avgörande för att GDPR inte ska fortsättas upplevas som ett hinder

I årsrapporten 2023 lyfte dataskyddsombudet att det inom Staden generellt bedömdes finnas en uppfattning om att det är omöjligt att följa GDPR och samtidigt driva den digitala utvecklingen framåt. Dataskyddsombudets upplevelse, utifrån de dialoger som varit under 2024, är att denna uppfattning fortfarande kvarstår och är något som i hög grad påverkar dataskyddsarbetet negativt. Dataskyddsombudet har i möten med funktioner från olika verksamheter inom Staden kontinuerligt fått höra att GDPR är något som är jobbigt och krångligt, och som blir ett hinder som försvårar deras arbete med att ta i bruk nya digitala lösningar. Som regel uttrycks detta efter eller precis inför att verksamheten ska teckna avtal, eller precis står inför att börja använda en ny digital lösning eftersom det ofta är först då som dataskyddsperspektivet beaktas. Dataskyddsombudet förstår att medarbetare i den situationen upplever GDPR som ett hinder, men ser samtidigt att GDPR inte kan klandras för de uppenbara brister i den interna styrningen som medfört att verksamheten inte arbetat med dataskyddsfrågorna i tid.

För att känslan av GDPR som något jobbigt och ett hinder inte ska fortsätta ha en negativ påverkan på dataskyddsarbetet behöver Staden som helhet arbeta för att öka medvetenheten om syftet med lagstiftningen. En del kan göras genom utbildningar, men centralt är också att det från ledningshåll inom stadens verksamheter börjar signaleras att dataskydd är något som ska beaktas och arbetas med. I den offentliga debatten hör man ofta representanter från näringslivet tala om att det offentliga måste vara modiga och testa nya saker. Dataskyddsombudets uppfattning att det modiga i dessa fall ofta handlar om att utmana den lagstiftning som styr offentlig sektor, till exempel då lagstiftningen begränsar möjligheterna att dela och/eller använda data. Lagstiftningen, inkluderat GDPR, utmålas då som ett administrativt hinder som hämmar utvecklingen. Denna bild av GDPR som ett hinder delas inte av dataskyddsombudet eftersom det inte finns någon motsättning mellan att följa lagkraven och samtidigt driva digitaliseringen framåt. Utifrån den

diskurs som råder bedömer dataskyddsombudet att det är viktigt att man på ledningsnivå har kunskap om syftet med GDPR och förståelse för att om GDPR sätter ”stopp” för en behandling eller en tjänst så finns det ett gott skäl till det. I praktiken innebär det att man på ledningsnivå behöver ta ansvar för att inte använda en digital tjänst eller inleda en behandling av personuppgifter som inte är förenlig med kraven i GDPR. En viktig del i detta är att ledningen börjar signalera en förväntan på att nya digitala lösningar ska vara långsiktigt hållbara, även utifrån ett integritetsperspektiv. På så sätt behöver verksamheter tänka på dataskydd tidigt i processen och kan förhoppningsvis undvika att hamna i situationer där GDPR enbart ses som något jobbigt eller ett administrativt hinder. Genom att integrera dataskyddsperspektivet från start i arbetet med nya tjänster och/eller vid utvecklandet av nya arbetssätt kan verksamheter hitta stabila och långsiktiga alternativ där människors grundläggande fri- och rättigheter inte äventyras. Något som blir, om möjligt, extra viktigt i takt med att användningen av ny teknik och AI ökar inom Stadens verksamheter.

2.1.3 Bristande ansvarstagande i Stadens arbete med AI medför risker för både enskilda och verksamheter

Fokus på ny teknik och AI har en enorm potential för att göra våra liv bättre, men den digitala utvecklingen blir inte hållbar utan begränsningar. Utan tydlig styrning i arbetet med digital innovation är risken att det går fort och att man i sin iver att röra sig framåt glömmer att hänsyn behöver tas till den personliga integriteten och att personuppgifter behandlas på ett korrekt sätt. Som en stor offentlig aktör har Göteborgs Stad att förvalta alla invånare och besökares förtroende. Oavsett om det handlar om elever, vårdnadshavare, anställda, brukare inom socialtjänst, eller någon annan kategori av kommuninvånare, så ska man kunna känna sig trygg med att användandet av innovativ teknik sker med respekt för den personliga integriteten och de regelverk som finns för att skydda enskildas personuppgifter.

Under året har dataskyddsombudet kunnat se att allt fler verksamheter inom Staden börjar utforska användningen av AI. Dataskyddsombudet har under året löpande kunnat identifiera stora risker med det arbete som bedrivs på stadenövergripande nivå. Riskerna kommer dels utifrån att det från centralt håll hittills saknas styrning och samordning i hur tekniken kan, och får, användas, dels utifrån att de tekniska lösningar som har lanserats ej först kontrollerats utifrån ett informationssäkerhets- och dataskyddsperspektiv. Dataskyddsombudets bedömning är att stadsledningskontoret och Intraservice behöver ta ett större ansvar i hanteringen av dessa risker, eftersom de båda verksamheterna är starkt drivande i användningen av AI inom Staden. Särskilda rekommendationer ställs därför till de båda verksamheterna i deras respektive årsrapporter.

Dataskyddsombudet vill utifrån identifierade risker med de stadenövergripande AI-lösningar som idag finns tillgängliga inom Staden (M365 Copilot i Edge, Svea GPT etc.) betona vikten av att förvaltningar och bolag innan en ny AI-lösning tas i bruk först kontrollerar så att denna är säkerställd utifrån ett informationssäkerhets- och dataskyddsperspektiv.

3 Dataskyddsombudets iakttagelser 2024

3.1 Verksamhetens dataskyddsarbete

Under 2024 har förvaltningen etablerat en intern dataskyddsorganisation. Att dataskyddskontakterna nu finns inom Enheten för styrning och uppföljning av informationssäkerhet bedömer dataskyddsombudet vara positivt, eftersom det ger förvaltningen en möjlighet att hantera dataskyddsfrågorna tillsammans med övriga informationssäkerhetsfrågor. För att den interna dataskyddsorganisationen nu ska kunna börja arbeta kvalitativt med dataskydd behöver medarbetare inom enheten utbildas och få utökade kunskaper i dataskydd. Medarbetare inom enheten rekommenderas därför avsätta tid och prioritera att delta vid de utbildningar, informationsinsatser etcetera som dataskyddsombudet tillhandahåller med syftet att utveckla och fördjupa sina kunskaper i dataskydd.

När det gäller utformningen av det interna dataskyddsarbetet behöver enheten börja med att ta fram en struktur för hur dataskyddsarbetet ska bedrivas inom förvaltningen. Det handlar om att ta fram interna arbetssätt och styrdokument för hanteringen av till exempel behandlingsregister och konsekvensbedömningar, att genomföra utbildningar för att öka den allmänna kunskapsnivån och om att integrera dataskyddsperspektivet i befintliga processer. Dataskyddsombudet upplever att fokus hittills främst riktats mot tjänsteleveransen, vilket medfört att man inte arbetat med förvaltningens interna riskfyllda behandlingar kopplat till exempelvis HR (medarbetarundersökningar, rehabilitering m.m.) och säkerhet (säkerhetsprövningar, kamerabevakning m.m.). Här är det viktigt att den interna dataskyddsorganisationen nu breddar sitt perspektiv och även börjar inventera och dokumentera de interna personuppgiftsbehandlingarna som inte är kopplade till tjänsteleveransen. Eftersom ett behandlingsregister utgör grunden för ett systematiskt dataskyddsarbete är det viktigt att förvaltningen prioriterar arbetet med detta, och inom ramen för det fortsätter lyfta frågan om personuppgiftsansvar för olika personuppgiftsbehandlingar. Under året har dataskyddsombudet deltagit och varit rådgivande i dialoger inom förvaltningen samt med stadsledningskontoret i ansvarsfrågan. Dataskyddsombudets uppfattning är att Intraservice i detta arbete haft en ledande roll och tagit på sig ansvar för att, i samverkan med dataskyddsombudet, driva frågan om ansvarsförhållanden för hela Stadens räkning.

Även om det nu finns en intern dataskyddsorganisation vill dataskyddsombudet särskilt påpeka att denna inte ensamt kan ta ansvar för hela förvaltningens dataskyddsarbete. För att göra dataskyddsarbetet hanterbart behöver förvaltningens olika avdelningar börja dokumentera information om behandlingar, tjänster och system (informationsbärare) på ett enhetligt sätt så att den interna dataskyddsorganisationen får en helhetsbild. Denna typ av grundläggande dokumentation om behandlingar såväl som tjänster är nödvändig för att den interna dataskyddsorganisationen ska kunna arbeta med frågorna och säkerställa att

nämnden uppfyller sina skyldigheter i egenskap av såväl personuppgiftsansvarig som personuppgiftsbiträde.

När det gäller i vilken utsträckning som dataskyddsombudet involverats i dataskyddsfrågor varierar detta mellan avdelningarna. Under året har dataskyddsombudet engagerats i arbetet med olika typer av frågeställningar, bland annat kopplat till kravställning vid upphandling, utformning av information till registrerade, hantering av personuppgiftsincidenter och genomförande av konsekvensbedömningar. Dataskyddsombudet har även varit aktiv och rådgivande i olika arbetspaket inom projektet Etablera systematiskt informations-säkerhetsarbete (ESI). Under 2024 har dataskyddsombudet särskilt noterat en ökad aktivitet och även upplevt en ökad medvetenhet i frågorna hos medarbetare inom avdelningen för gemensamma tjänster och då särskilt verksamhetsområdena HR och Ekonomi. Dataskyddsombudet har under året sett en positiv utveckling i hur dataskyddsfrågor hanteras i tjänsteleveransen inom dessa områden och vill därför särskilt lyfta fram dessa verksamhetsområden som goda exempel.

Sammantaget upplever dataskyddsombudet att förvaltningen som helhet börjat arbeta mer aktivt med dataskyddsfrågor under 2024. Den ökade aktiviteten bedöms till stor del bero på det arbete som utförs inom ramen för ESI-projektet.

3.2 Särskilda iakttagelser

3.2.1 Brister i tjänsteleveransen kvarstår

I årsrapporten för 2023 lyfte dataskyddsombudet de risker som identifierats kopplat till brister i förvaltningens tjänsteleverans när det gällde att säkerställa att de tjänster/den digitala infrastrukturen som levereras uppfyller gällande lagkrav. Precis som för föregående år kan dataskyddsombudet konstatera att förvaltningen även under 2024 har fortsatt att utveckla och leverera tjänster/digitala lösningar utan att dessa först kontrollerats utifrån ett dataskydds- och informationssäkerhetsperspektiv. Det tydligaste exemplet på detta under 2024 är aktiveringen av Microsoft Copilot i Edge, vilket gjordes utan genomförande av tillräckliga riskbedömningar eller involvering av dataskyddsombudet. När dataskyddsombudet kontaktade ansvariga inom förvaltningen för att få ta del av underlag visades det att underlag saknades och att de frågor som dataskyddsombudet ställde ej kunde besvaras.

Dataskyddsombudets förhoppning är att det arbete som pågår inom ESI-projektet med att ta fram nya arbetssätt och styrdokument kopplat till informationssäkerhet ska kunna bidra till att hantera bristerna. För att ESI-projektets arbete ska få genomslag krävs dock även att man inom förvaltningen börjar arbeta aktivt med att bryta de vanor och förhållningssätt som bidrar till en leverans av osäkra tjänster/digitala lösningar. Dataskyddsombudet har i tidigare årsrapporter rekommenderat förvaltningen att internt tydliggöra att det inte är valfritt för medarbetare att följa de lagar och regler som gäller för verksamheten, och utifrån gjorda iakttagelser under året bedöms det även fortsatt finnas behov av detta.

Utifrån gjorda iakttagelser är dataskyddsombudets uppfattning att frågan särskilt behöver arbetas med inom avdelningen för Digital infrastruktur.

3.2.2 Bristande ansvarstagande i Stadens arbete med AI medför risker för både enskilda och verksamheter

Med Intraservices uppdrag att pådriva användningen av AI i Göteborg Stad, kommer också ett ansvar för att säkerställa att arbetet bedrivs utifrån de regler och krav som styr verksamheterna som påverkas. Utifrån gjorda iakttagelser under året är dataskyddsombudets uppfattning att dataskyddsperspektivet genomgående saknas i det AI-arbete som under året har bedrivits av eller inom förvaltningen.

Identifierade risker inom förvaltningens AI-arbete

Det dataskyddsombudet bedömer särskilt allvarligt är att det under året startats och/eller genomförts AI-projekt utan att grundläggande frågor kopplat till ansvar och avtal utretts. Dataskyddsombudets bedömning är att detta beror på att det inom ansvariga delar av förvaltningen saknas grundläggande kunskaper kopplat till dataskydds- och AI-lagstiftningen, vilket har medfört att frågorna inte kunnat hanteras inom ramen för projekten. I stället har fokus varit att komma igång snabbt och att ”våga testa”, trots att man inte haft koll på de rättsliga förutsättningarna. Då denna inställning varit återkommande inom olika projekt är dataskyddsombudets bedömning att förvaltningen brustit i att ta sitt ansvar i dessa frågor.

Dataskyddsombudet har under året vid flera tillfället lyft de risker som identifierats till ansvariga funktioner inom förvaltningen. Vid de dialoger som varit upplever dataskyddsombudet att det finns en samsyn i frågan, och ansvariga funktioner har efterfrågat stöd i deras arbete. Dataskyddsombudet har utifrån det deltagit vid och lämnat råd inom ramen för olika forum (t.ex. AI-forum, AI-speedar och Lärlabb) som arrangerats under året. Dock bedömer dataskyddsombudet, utifrån de iakttagelser som gjorts, att ansvariga funktioner inom förvaltningen behöver stöd i mer än dataskyddsfrågorna för att kunna komma till rätta med de brister som identifierats. Det handlar särskilt om stöd i övriga juridiska frågor (avtal, offentlighet- och sekretess m.m.) och informationssäkerhet (kopplat till de AI-lösningar som ”marknadsförs” av förvaltningen).

När det gäller juridiska frågor är dataskyddsombudets uppfattning att förvaltningen hittills främst förlitat sig på de juridiska bedömningar som gjorts av AI Sweden inom ramen för de AI-projekt/samarbeten som förvaltningen har med AI Sweden. Detta bedömer dataskyddsombudet vara problematiskt eftersom de funktioner som arbetar med AI inom förvaltningen inte har rätt kompetens för att kunna granska de underlag/bedömningar som görs. Dataskyddsombudet har också vid flera tillfällen ifrågasatt gjorda bedömningar och har vid olika mötesforum behövt bemöta det som kommunicerats från representanter från AI Sweden utifrån att informationen varit direkt felaktig. Då dataskyddsombudet ser stora risker med att felaktig information om hur AI-lösningar kan användas sprids till medarbetare inom olika verksamheter i Staden rekommenderas förvaltningen omgående vidta åtgärder för

att säkerställa att externa parter inte tillåts fortsätta kommunicera missvisande information vid de AI-forum som förvaltningen arrangerar. Ytterligare en viktig åtgärd är att ansvariga för AI-arbetet börjar involvera förvaltningsjuristerna i arbetet med frågorna. Dels för att stämma av innehåll i avtal och juridiska ställningstaganden, dels för att få stöd i att identifiera vilka regelverk som påverkar om/hur en AI-tjänst är möjlig att använda.

När det gäller informationssäkerhet så har dataskyddsombudet under året kunnat konstatera att förvaltningen ”marknadsför” AI-lösningar utan att dessa är kontrollerade utifrån ett dataskydds- och informationssäkerhetsperspektiv. Då förvaltningen bedöms ha ett stort förtroendekapital i AI-frågor inom stadens olika verksamheter är detta problematiskt eftersom medarbetare förutsätter att de tjänster som kommuniceras är säkra att använda. Här bedöms förvaltningen behöva ta ett större ansvar för att enbart kommunicera och lyfta fram AI-lösningar som det finns avtal med och som är godkända för användning utifrån ett dataskydds- och informationssäkerhetsperspektiv.

Framtidens digitala assistent för offentlig sektor

Intraservice har under året varit samordnande inom Staden för projektet Framtidens digitala assistent för offentlig sektor, etapp 1, som leds av AI Sweden. Projektet syftar till att undersöka förutsättningarna för en nationell AI-lösning för text i offentlig sektor. Dataskyddsombudets uppfattning är att Intraservice har en ledande roll i arbetet.

Utifrån den dialog som varit under 2024 kan dataskyddsombudet konstatera att det inom förvaltningen saknas styrning och samordning kring projektet kopplat till dataskyddsfrågorna. Det är flera frågor som borde ha utretts innan den aktuella AI-lösningen togs i bruk. Det handlar till exempel om att identifiera och dokumentera vilka personuppgiftsbehandlingar som aktualiseras och att bedöma ansvars-förhållanden mellan utvecklarorganisationen, Intraservice och övriga förvaltningar. Dataskyddsombudet bedömer att det, utifrån hur projektet har bedrivits inom förvaltningen, finns uppenbara risker att personuppgifter inte behandlas på ett korrekt sätt. Särskilt allvarligt är att förvaltningen initierat och genomdrivit ett helt projekt utan att nödvändiga avtal för reglering av ansvarsförhållanden utifrån GDPR funnits på plats. Det är även anmärkningsvärt att förvaltningen fortsatt initiera etapp 2 av projektet under samma förutsättningar.

Dataskyddsombudet rekommenderar förvaltningen att snarast påbörja arbetet med att kartlägga och utreda ansvarsförhållanden gentemot övriga aktörer inom projektet, vilka personuppgiftsbehandlingar som aktualiseras och utifrån den samlade dokumentationen bedöma om en konsekvensbedömning behöver göras. Förvaltningen behöver även säkerställa att nödvändiga avtal upprättas utifrån resultatet av ansvarsbedömningen.

Dataskyddsombudet avråder förvaltningen från att fortsätta och/eller inleda, eller möjliggöra, nya behandlingar av personuppgifter i Svea GPT innan de juridiska förutsättningarna för detta har utretts och bedömts.

4 Granskning av dataskyddsarbetet 2024

4.1 Fördjupad kontroll 2024

Under våren 2023 genomförde dataskyddsenheten en informationsinsats med fokus på behandlingsregistret enligt artikel 30 i GDPR. Som uppföljning på denna informationsinsats genomförde dataskyddsenheten under hösten 2024 en fördjupad kontroll med fokus på behandlingsregistret för ett antal av stadens verksamheter (dock ej inom aktuell verksamhet).

Resultatet av kontrollen visade sammantaget på stora brister i omhändertagandet av artikel 30 i GDPR. För att alla verksamheter i Staden ska få ta del av resultaten från kontrollen har dataskyddsombudet tagit fram en stadengemensam rapport. Den stadengemensamma rapporten innehåller både generella iakttagelser från kontrollen, dataskyddsombudets bedömningar i olika sakfrågor och konkreta exempel på hur behandlingsregistret kan utformas med hänvisningar till olika rättskällor som dataskyddsombudet anser har ett generellt värde för hela Staden. Rapporten blir en form av ytterligare vägledning avseende hur arbetet med behandlingsregistret kan utformas för att skapa förutsättningar för ett funktionellt dataskyddsarbete där kraven i artikel 30 i GDPR kan uppfyllas.

Dataskyddsombudet kommer under 2025 följa upp dels att samtliga av Stadens verksamheter har tagit del av rapporten, dels hur verksamheterna avser omhänderta de generella rekommendationerna i arbetet med det egna behandlingsregistret.

4.2 Uppföljning av lämnade rekommendationer

4.2.1 Uppföljning av verksamhetens arbete med rekommenderade fokusområden 2024

Dataskyddsombudet har följt upp hur verksamheten arbetat med de fokusområden som rekommenderades för 2024.

Fokusområde 1: Dataskyddsorganisation

Verksamheten gavs följande rekommendationer:

- Fastställ och tillsätt en intern dataskyddsorganisation, med tillräckliga resurser, mandat och kompetens, som kan samordna och arbeta med frågorna inom förvaltningen.

Kommentarer och rekommendationer

Uppföljningen visar att förvaltningen under 2024 etablerat en intern dataskyddsorganisation. Strukturen för den interna dataskyddsorganisationen fastställdes av nämnden i juni 2024 och innebär att befintliga roller inom Enheten för styrning och uppföljning av informationssäkerhet får utökade samt nya ansvar kopplat till aktiviteter bland annat gällande dataskydd. Från september månad utgör medarbetare inom enheten dataskyddskontakter och har därför huvudansvar för dialogen med dataskyddsombudet. Tanken är att dataskyddskontakterna ska vara en ”SPOC” (Singel Point Of Contact) för alla typer av ärenden rörande dataskydd. När det gäller att säkerställa att medarbetare har kompetens anger förvaltningen anger att det under perioden september till november genomförts utbildningar, men ifall dessa har inkluderat dataskydd framgår inte.

Förvaltningen anger vidare att etableringen av den interna dataskyddsorganisationen är en del i den organisationsstruktur med processer och arbetssätt som håller på att byggas upp, vilken ska styra och stödja arbetet med informationssäkerhet inom förvaltningen. Fortsatt arbete med andra ansvar/roller/mandat kommer att ske löpande inom ESI-projektet.

Det är positivt att förvaltningen under 2024 har fastställt en intern dataskyddsorganisation, men för att denna ska få genomslag och kunna bidra till att stärka förvaltningens dataskyddsarbete behöver ytterligare arbete göras. Det behöver tas fram interna arbetssätt, rutiner och rollbeskrivningar som tydliggör dataskyddskontakternas uppdrag och ansvar i olika dataskyddsfrågor. Utifrån förvaltningens uppdrag som intern tjänsteleverantör handlar det både om dataskyddsfrågor relaterade till tjänsteleveransen och till det interna arbetet inom förvaltningen. Dataskyddsombudet kan konstatera att det är ett omfattande ansvar som nu åligger enheten och det är därför viktigt att förvaltningen tillser att enheten ges tillräckliga resurser samt tillhandahåller det underlag (i form av information, dokumentation etc.) som krävs.

Utifrån att den interna dataskyddsorganisationen fortfarande är ny, och under utveckling, kommer dataskyddsombudet att fortsätta följa upp förvaltningens arbete med rekommendationerna under 2025.

Dataskyddsombudets iakttagelser avseende förvaltningens dataskyddsarbete under 2024 redogörs för under avsnitt 3.1 i rapporten.

Fokusområde 2: Register över personuppgiftsbehandlingar

Verksamheten gavs följande rekommendationer:

- Ta fram ett personuppgiftsbehandlingsregister. Gå igenom verksamhetens personuppgiftsbehandlingar, se över hur dessa ska definieras och dokumentera respektive behandling utifrån kraven enligt artikel 30 i GDPR.

<u>Kommentarer och rekommendationer</u>

I uppföljningen hänvisar förvaltningen till det arbete som bedrivs inom ramen för ESI-projektet. I projektet ingår att se över hantering av behandlingsregistret,

processer och arbetssätt tillhörande dokumentation av personuppgiftsbehandlingar. Det har även upphandlats ett nytt systemstöd för bland annat behandlingsregister som implementeras under Q1 2025, och Intraservice kommer att vara en av de första förvaltningarna som kommer att starta upp sitt införandeprojekt vilket innebär att förvaltningens personuppgiftsregister upprättas i systemstödet. Vidare anges att det pågår ett arbete med att dokumentera personuppgiftsbehandlingar tillhörande tjänsteleveranser inkluderar framtagande av tjänstespecifikationer och funktionsbeskrivningar. Beräknad tidsperiod för åtgärder kopplade till huvudpaket Systemstöd (inkl. PU-reg.) är 2023-10-01 – 2025-06-30.

När det gäller det behandlingsregister som förvaltningen ska upprätta i egenskap av personuppgiftsansvarig är dataskyddsombudets bedömning att det fortfarande kvarstår ett stort arbete. Hittills har fokus varit på en väldigt begränsad del av förvaltningens verksamhet – kopplat till informationssäkerhet – medan övriga delar har utelämnats. För att komma vidare i arbetet bör förvaltningen nu fokusera på andra delar där det är tydligt att förvaltningen har ett eget personuppgiftsansvar till exempel inom HR, fysisk säkerhet (kamerabevakning) eller kopplat till kansliet (diarieföring, utlämning av allmän handling etc.). För att förvaltningens arbete med behandlingsregistret ska bli hanterbart behöver det brytas ner i olika delar, förslagsvis utifrån förvaltningens klassificeringsstruktur. Genom att utgå från den kan förvaltningen få en bra överblick av verksamheten som helhet, för att därefter kunna gå igenom respektive verksamhetsområde och identifiera behandlingar. I arbetet är det viktigt att förvaltningen skiljer på det register som ska upprättas i egenskap av personuppgiftsansvarig respektive personuppgiftsbiträde, så att det blir tydligt – både inom verksamheten och gentemot registrerade – vilket ansvar som förvaltningen har.

Utifrån att ett behandlingsregister fortfarande saknas, och införandet av ett systemstöd inte per automatik innebär att ett behandlingsregister upprättas, gör dataskyddsombudet bedömningen att förvaltningen under 2024 ej omhändertagit de rekommendationer som lämnats. Fortsatt uppföljning kommer därför göras 2025.

Fokusområde 3: Informationsplikt

Verksamheten gavs följande rekommendationer:

- Se över samtliga delar i den information som lämnas till de registrerade och de arbetssätt som tillämpas för att säkerställa att informationsplikten gentemot de registrerade uppfylls. I arbetet behöver de rekommendationer som tidigare lämnats kopplat till den specifika informationen i integritetspolicyn omhändertas.

<u>Kommentarer och rekommendationer</u>

I uppföljningen anges att aktiviteter tillhörande kontrollpunkt 7, Informationsplikt, väntar på att prioriteras och planeras in för omhändertagande under perioden december 2024 – januari 2025 inom ramen för ESI-projektet.

Då förvaltningen under 2024 inte har arbetat aktivt med frågan och därmed ej vidtagit några åtgärder för att hantera de rekommendationer som lämnades i årsrapporten 2023 kvarstår dessa för 2025.

Dataskyddsombudet vill också särskilt lyfta att en förutsättning för att förvaltningen ska kunna uppfylla sina skyldigheter utifrån informationsplikten är att förvaltningen har kunskap om vilka personuppgiftsbehandlingar som utförs inom verksamheten. Arbetet med informationsplikten är därför beroende av att det finns ett behandlingsregister. Med anledning av detta rekommenderas förvaltningen att under 2025 prioritera arbetet med behandlingsregistret framför informationsplikten.

4.2.2 Uppföljning av särskilda iakttagelser

Särskilda iakttagelser (2021): Intraservices hantering av personuppgiftsincidenter

Verksamheten gavs följande rekommendationer:

- Att göra en översyn av rutiner och processer för att säkerställa att incidenter inte missas.
- Ta fram tydliga instruktioner för vilken information som ska kommuniceras till PUA vid incidenter.
- Säkerställa tillräcklig kompetens och möjlighet till utbildning hos berörda parter (medarbetare).

Kommentarer och rekommendationer

Uppföljningen 2023 visade att förvaltningen hade arbetat med frågan och att flera åtgärder hade vidtagits, men att det kvarstod risker kopplat till själva incidenthanteringsprocessen, den låga kunskapsnivån inom förvaltningen som helhet samt kopplat till dokumentationen av incidenter. Av uppföljningen 2024 framgår att förvaltningen fortsatt arbetet med incidenthantering inom ramen för ESI-projektet. Inom ramen för projektet har analyser genomförts, vilka medfört förslag till justeringar i incidenthanteringsprocessen, bland annat gällande arbetssätt för att identifiera och hantera personuppgiftsincidenter.

Delar som justerats under året är vilka kontaktvägar till personuppgiftsansvariga förvaltningar och bolag som används vid inträffade incidenter, genomförandet ”lessons learned” vid större incidenter samt uppdatering av mallar och dokument för att uppfylla dokumentationskraven vid anmälan av incidenter till Integritetsskyddsmyndigheten (IMY). Utöver det har utbildningar genomförts för handläggare och dokumentationen kring hanteringen av incidenter har uppdaterats så att den nu även omfattar brist på tillgänglighet (tillgänglighet enligt för kunden gällande Service Level Agreement (SLA)). Vidare anger förvaltningen att fortsatt arbete med incidentprocessen kommer att fortsätta inom ramen för ESI-projektet.

Dataskyddsombudet är positiv till de ändringar som genomförts under 2024, men kan utifrån gjorda iakttagelser under året konstatera att ytterligare åtgärder krävs för att förvaltningens incidenthantering ska bli ändamålsenlig.

Under 2024 har dataskyddsombudet kunnat se att förvaltningens hantering av mindre personuppgiftsincidenter förbättrats, och dataskyddsombudet vill därför särskilt lyfta fram att det är positivt att man inom både it-supporten (Servicecenter) och avdelningen för gemensamma tjänster fått in arbetssätt för att upptäcka och anmäla incidenter. Det som förvaltningen däremot behöver fortsätta arbeta med är hanteringen av större personuppgiftsincidenter, då hanteringen vid dessa tillfällen genomgående brustit under året. Förvaltningen bedöms därför behöva fortsätta arbetet med att se över rutiner och processer för incidenthanteringen med fokus på de incidenter som omfattar mer än en verksamhet.

En grundläggande förutsättning för att personuppgiftsincidenter ska kunna hanteras är att medarbetare inom förvaltningen har kunskap om vad en personuppgiftsincident är och därför kan identifiera när en inträffar. Under året har det vid flera tillfällen hänt att incidenter ej upptäcks på grund av bristande kunskap hos enskilda medarbetare. I vissa fall är det först efter att dataskyddsombudet och/eller berörda verksamheter tagit kontakt och uppmärksammat förvaltningen på det inträffade som incidentprocessen startats. Särskilt allvarligt har det varit när det inträffat incidenter inom de system som förvaltningen levererar till socialförvaltningarna.

Utifrån gjorda iakttagelser under året är dataskyddsombudets bedömning att de rekommendationer som lämnades i årsrapporten 2023 gällande incidentprocessen och den låga kunskapsnivån inom förvaltningen fortfarande kvarstår. Förvaltningen rekommenderas därför omhänderta dessa i arbetet med incidenthanteringen inom ramen för ESI-projektet. Vidare, utifrån att bristerna i förvaltningens incidenthantering bedöms kunna medföra höga risker för registrerade, har dataskyddsombudet valt att ha personuppgiftsincidenter som ett rekommenderat fokusområde för 2025. Detta innebär att dataskyddsombudet under året löpande kommer följa upp hur arbetet med att omhänderta rekommendationerna fortskrider.

5 Rekommenderade fokusområden 2025

Dataskyddsombudet rekommenderar, utifrån gjorda iakttagelser och resultaten av uppföljningen, verksamheten att under 2025 fortsätta prioritera arbetet med två av de kontrollpunkter som rekommenderades för 2024. Utöver dessa rekommenderas förvaltningen även prioritera arbetet inom ett område där dataskyddsombudet tidigare år lämnat särskilda rekommendationer. De rekommenderade fokusområdena listas i punktform enligt nedan.

Detta är områden som dataskyddsombudet särskilt kommer att följa upp under året. Uppföljningen kommer ske kontinuerligt under avstämningsmöten med verksamheten, och inom ramen för den uppföljning som dataskyddsombudet genomför under hösten 2025.

Förvaltningen rekommenderas 2025 prioritera följande delar av dataskyddsarbetet:

- Kontrollpunkt 1: Dataskyddsorganisation

Ta fram interna arbetssätt, rutiner och rollbeskrivningar som tydliggör dataskyddskontakternas uppdrag och ansvar i olika dataskyddsfrågor.

- Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Ta fram ett behandlingsregister. Identifiera de personuppgiftsbehandlingar som ligger inom nämndens ansvar, se över hur dessa ska definieras och dokumentera respektive behandling utifrån kraven enligt artikel 30 i GDPR.

I arbetet rekommenderas förvaltningen ta del av den generella granskningsrapporten från dataskyddsombudets fördjupade kontroll och se över behandlingsregistret utifrån rekommendationerna som framgår av granskningsrapporten.

- Kontrollpunkt 2: Personuppgiftsincidenter

1. Gör en översyn av befintlig process för personuppgiftsincidenter med syftet att säkerställa att berörda funktioner involveras i ett tidigt skede i hanteringen.

2. Ta fram instruktioner för vad som ska kommuniceras till personuppgiftsansvariga när en incident inträffar, samt rutiner för när och hur kommunikationen ska ske.

3. Genomför utbildningsinsatser inom förvaltningen med syftet att öka medarbetares kunskaper om vad en personuppgiftsincident är och hur en incident ska hanteras.

6 Bilagor

Bilaga 1: Kontrollplan för dataskyddsarbetet 2024–2025