Yttrande

Moderaterna, Demokraterna, Liberalerna, Kristdemokraterna

2025-02-20

Yttrande angående Årsrapport för dataskyddsarbetet 2024 för kommunstyrelsen

Yttrandet

Nämnden för Intraservice hemställde under 2024 om att starta en hemtagning av Skatteverkets uppgifter i Navet till en server inom Göteborgs stad. I samband med hemställan efterfrågade Intraservice juridisk stöttning från Stadsledningskontoret. I årsrapporten för dataskyddsarbetet lyfts ärendet som ett exempel på där det var relevant för dataskyddsombudet att involveras. En sådan involvering uteblev dessvärre. Detta menar vi är exempel på hur dataskyddsarbetet i staden släpar efter. Funktionen finns för att stötta upp och motverka fel, men verkar till stor del inte användas.

För att motverka eventuellt dataintrång eller felaktig hantering av känsliga uppgifter behöver arbetet med dataskydd accelereras och värderas högre inom stadens verksamheter. Det är positivt att årsrapporten lyfter de åtgärder som tillsatts för att framåt involvera dataskyddsombudet i den interna ärendeberedningen på ett bättre sätt samt rutiner för hur dataskyddsombudet ska involveras i de olika processerna. Arbetet med att sätta rutiner och processer behöver komma på plats skyndsamt då hoten mot dataskyddet succesivt har ökat. I arbetet med att etablera processer behöver brister och eventuella hot identifieras för att möjliggöra åtgärdsprocesser.

Det är angeläget att dataskyddsarbetet fungerar och inkluderas i relevanta ärenden under de oroliga tider Göteborg och omvärlden befinner sig i. Därav ser vi positivt på att det nu skapas förutsättningar och processer för att accelerera arbetet med dataskydd i staden.

Tjänsteutlåtande
Utfärdat 2025-01-29
Ärendenummer SLK-2025-00134

Handläggare
Aya Norvell
Telefon: 031-368 01 90
E-post: aya.norvell@stadshuset.goteborg.se

Årsrapport för dataskyddsarbetet 2024 för kommunstyrelsen

Förslag till beslut

I kommunstyrelsen:

Årsrapport för dataskyddsarbetet 2024 för kommunstyrelsen antecknas.

Ärendet

Dataskyddsombudet lämnar årligen en rapport om verksamhetens dataskyddsarbete till varje nämnd och bolag i Göteborgs Stad. Rapporten redogör för det kontrollarbete som genomförts och de iakttagelser som gjorts. Årsrapporten är avsedd att kunna användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd.

Förutom att notera sina övergripande iakttagelser följer dataskyddsombudet upp verksamhetens dataskyddsarbete utifrån de tre fokusområden som föreslogs för 2024.

Stadsledningskontoret kommer i det fortsatta utvecklingsarbetet att utgå från lämnade rekommendationer, med start i de för förvaltningen mest angelägna åtgärderna. Rapporten följer även upp den granskning som gjordes 2023 och kontoret arbetar vidare med att hantera de rekommendationer som återstår.

Bilaga

Årsrapport för dataskyddsarbetet 2024

Aya Norvell
Chef för Kontorsledning

Eva Hessman
Stadsdirektör

Göteborgs Stad

Årsrapport för dataskyddsarbetet 2024

Kommunstyrelsen

2025-01-13

Innehåll

1 Dataskydd i kommunal verksamhet

Att få ta del av och hantera andra människors personliga uppgifter på ett sådant sätt som kommunala förvaltningar och bolag gör innebär att förvalta ett stort förtroende. 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

Dataskyddsombudet har under året haft en regelbunden dialog med förvaltningens dataskyddsorganisation och blivit involverad i arbetet med olika dataskyddsfrågor. Precis som föregående år upplevs samarbetet mellan dataskyddsombudet och den interna dataskyddsorganisationen fungera bra. Frågor som arbetats med under året gäller bland annat behandlingsregistret, tröskelanalyser och konsekvens-bedömningar, personuppgiftsincidenter och hanteringen av registrerades rättigheter. Utöver arbetet med den interna dataskyddsorganisationen har dataskyddsombudet även haft viss kontakt med funktioner inom förvaltningens olika verksamhetsområden i olika frågor till exempel kopplat till remisser, intern kontroll, inom HR och kommunikation samt informationssäkerhet och digitalisering. Dataskyddsombudet upplever att förvaltningens involvering av dataskyddsombudet i dataskyddsfrågor under året har ökat något, men då involveringen till stor del upplevs vara personberoende och skiljer sig mellan verksamhetsområdena, behöver förvaltningen fortsätta arbeta med att ta fram arbetssätt för hur och när dataskyddsombudet ska kontaktas.

Under året har förvaltningen genomfört flera tröskelanalyser och konsekvensbedömningar. Även om underlagen varit av varierande kvalitet kan dataskyddsombudet se en positiv utveckling i förvaltningens underlag och arbetssätt. Det som förvaltningen bedöms behöva fortsätta arbeta med är att genomföra konsekvensbedömningar i tid, för att undvika att hamna i situationer där en behandling inleds innan dataskyddsombudet lämnat sina synpunkter. I samband med medarbetarundersökningen 2024 samlades en ny typ av känsliga personuppgifter in av förvaltningen, vilket krävde en uppdatering av befintlig konsekvensbedömning. Dataskyddsombudet fick ta del av konsekvens-bedömningen precis innan medarbetarenkäten skickades ut och utifrån den snäva tidsramen hann förvaltningen inte färdigställda konsekvensbedömningen innan dess att medarbetarenkäten genomfördes. I praktiken innebar det att stadsledningskontoret innan behandlingen inleddes inte kunde säkerställa att denna var laglig eller att skyddet för de registrerade var tillräckligt. Konsekvensen är att kommunstyrelsen för denna behandling inte uppfyllt sina skyldigheter enligt dataskyddsförordningen. Då det gäller en personuppgiftsbehandling som omfattar samtliga anställda inom Stadens förvaltningar och ett antal bolag ser dataskyddsombudet anledning att informera kommunstyrelsen i frågan.

3.2 Särskilda iakttagelser

3.2.1 Etablering av ny central dataskyddsfunktion

Under hösten har den nya dataskyddsfunktionen etablerats på stadsledningskontoret. Dataskyddsombudet och dataskyddsfunktionen har under hösten inlett ett samarbete och kommer framåt ha en fortsatt nära samverkan. Det är mycket positivt att stadsledningskontoret nu tar ett större ansvar för att styra och samordna Stadens dataskyddsarbete. Genom den nya funktionen har stadsledningskontoret stora möjligheter att bidra till ett stärkt dataskydd inom Staden som helhet.

Då dataskyddsfunktionen tillhör stadsledningskontoret kommer uppföljning av funktionens arbete att göras inom ramen för kommunstyrelsens ansvar under 2025.

3.2.2 Risker kopplat till att dataskyddsombudet ej involveras och/eller utestängs

I årsrapporten 2023 lyfte dataskyddsombudet risker kopplat till bristande kunskaper inom dataskydd som innebar att dataskyddsombudet ej involverades i, och/eller utestängdes, från förvaltningens arbete. Bristerna bedömdes vara genomgående inom förvaltningens olika delar, men särskilt allvarliga inom områdena för Ärende och utredning samt Digitalisering och innovation. Dataskyddsombudet lyfte i årsrapporten även att det under åren förekommit flera situationer där olika funktioner från förvaltningen lämnat felaktiga råd och/eller information utifrån dataskyddslagstiftningen till bolag och förvaltningar i Staden. Utifrån detta rekommenderades förvaltningen att vidta ett antal åtgärder för att öka den allmänna kunskapsnivån i dataskydd inom förvaltningen, och av uppföljningen (se avsnitt 4.2.1) framgår att förvaltningen under året arbetat med frågan.

Inom ärendeberedningen och i utredningsarbetet

Under 2024 har dataskyddsombudet blivit involverad i förvaltningens besvarande av statliga remisser i det fall dessa har en påverkan på dataskyddet, till exempel kopplat till kamerabevakning och informationsdelning. Det är positivt att förvaltningen nu börjat involvera dataskyddsombudet i vissa delar av ärendeberedningen. Framåt behöver förvaltningen även se över hur verksamheten kan involvera dataskyddsombudet i den interna ärendeberedningen till kommunstyrelsen och fullmäktige när det gäller utredning av politiska yrkanden eller andra beslutsunderlag som inkluderar integritets- och dataskyddsfrågor.

Ett konkret exempel på när förvaltningen borde ha involverat dataskyddsombudet under året är i hanteringen av ärendet ”Hemställan från nämnden för Intraservice att utreda personuppgiftsansvaret i samband med och efter en hemtagning av Skatteverkets uppgifter i Navet till en server inom Göteborgs Stad” (SLK-2023-01098), eftersom det tydligt gäller dataskydd. Dataskyddsombudets uppfattning är att stadsledningskontoret egentligen borde ha involverat och rådfrågat

dataskyddsombudet redan när ärendet först behandlades under 2023, och att de juridiska frågeställningar som under 2024 lyfts av Intraservice borde ha utretts av stadsledningskontoret innan dess att beslut fattades och uppdraget tilldelades. Vidare är dataskyddsombudets bedömning att denna hantering, där beslutsunderlag tas fram utan att dataskyddsperspektivet omhändertagits, är ett återkommande problem inom stadsledningskontorets ärendeberedning. Att stadsledningskontoret inte tar ansvar för att lyfta och/eller utreda denna typ av juridiska frågeställningar bedöms vara en allvarlig brist utifrån de risker detta medför för såväl registrerade som verksamheter.

Sammantaget bedöms stadsledningskontoret under 2024 inte ha kunnat säkerställa att dataskyddsombudet involveras i ärendeberedningen, med konsekvensen att kommunstyrelsen inte uppfyllt sina skyldigheter enligt dataskyddslagstiftningen. Förvaltningen rekommenderas därför att se över hur dataskyddsombudet framåt kan involveras i den interna ärendeberedningen inom ramen för arbetet med att kartlägga processer och ta fram rutiner för hur dataskyddsombudet ska involveras i de olika processerna (se avsnitt 4.2.1 ”Dataskyddsorganisation”).

Inom arbetet med digitalisering och innovation

I årsrapporten 2023 lyfte dataskyddsombudet att en genomgående brist i styrningen av Stadens digitaliserings- och innovationsarbete var att dataskyddsperspektivet saknades och att dataskyddsombudet inte involverades i arbetet.

Under våren har dataskyddsombudet varit med i förvaltningens arbete med budgetuppdraget att utreda hur AI-funktioner kan automatisera och effektivisera arbete som utförs i Göteborgs Stad. Dataskyddsombudets involvering i arbetet kom först efter att dataskyddsombudet själv kontaktat ansvariga och efterfrågat deltagande. Dataskyddsombudet har även efterfrågat samarbete med verksamheten i arbetet med att uppdatera ”Göteborgs Stads riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltning”, efter att ha fått information från en annan av Stadens förvaltningar om att ett arbete med personuppgiftsdelarna i denna pågick. Dataskyddsombudet kontaktade innan sommaren ansvarig för arbetet inom förvaltningen men fick ej något svar.

Utifrån gjorda iakttagelser bedömer dataskyddsombudet att förvaltningen under 2025 behöver vidta åtgärder för att involvera dataskyddsombudet och integrera dataskyddsfrågor i sitt digitaliserings- och innovationsarbete. Förvaltningen rekommenderas därför att se över hur dataskyddsombudet framåt kan involveras i arbetet med digitalisering och innovation inom ramen för arbetet med att kartlägga processer och ta fram rutiner för hur dataskyddsombudet ska involveras i de olika processerna (se avsnitt 4.2.1 ”Dataskyddsorganisation”).

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

Med stadsledningskontorets övergripande ansvar att driva digitalisering 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.

Budgetuppdrag kopplat till AI

Stadsledningskontoret och Intraservice har under 2024 tillsammans haft uppdraget att utreda hur AI-funktioner kan automatisera och effektivisera arbete som utförs i Göteborgs Stad. Uppdraget slutrapporterades i november genom rapporten ”Automatisering och effektivisering med hjälp av AI – slutrapport”. Dataskyddsombudet har tagit del av rapporten med fokus på de delar som gäller dataskydd och personlig integritet.

En balansakt som alltid behöver vara lagd till de registrerades fördel
I rapporten lyfts det fram att införandet av AI-system måste ske i enhetlighet med gällande lagstiftning, och att möjligheterna till effektivisering och automatisering behöver balanseras mot nödvändigheten att skydda individens rättigheter. Under avsnittet gällande juridik i rapporten lyfts de utmaningar som finns med att tillämpa flera regelverk parallellt, särskilt utifrån att viss lagstiftning är ny och vägledning saknas. Utifrån ett juridiskt perspektiv betonas även vikten av att genomföra och dokumentera de bedömningar som görs mellan risk och verksamhetsnytta, samtidigt som utmaningen i att anpassa lagstiftning och utveckling till varandra anges kunna innebära att ”våga” skapa ny praxis.

Även om det kan ses som en balansakt vill dataskyddsombudet vara tydlig med att balansen alltid behöver vara lagd till de enskilda registrerades fördel och aldrig får innebära att Staden tummar på det regelverk som finns till för att skydda personuppgifter. Dataskyddsombudet vill därför påminna förvaltningen om att Stadens verksamheter behöver följa dataskyddslagstiftningen på samma sätt som man behöver följa all annan lagstiftning.

Stort behov av ökad central styrning i AI-frågor inom Staden
I rapporten lyfts även behovet av en samlad AI-utveckling inom Staden fram, och att fokus bör riktas mot att samordna och koordinera insatser för att undvika en spretig och ineffektiv utveckling. Göteborgs Stad bedöms befinna sig i de tidiga faserna i AI-arbetet, och för att ta nästa steg bedöms staden behöva etablera arbetssätt och processer som stödjer en kontrollerad och hållbar utveckling.

Dataskyddsombudet delar bedömningen att Stadens arbete med AI behöver samordnas, men ser utöver det även ett starkt behov av ökad central styrning och delar inte bedömningen att det saknas behov av separata styrdokument för AI. Avsaknaden av styrning i AI-frågor har medfört att Stadens AI-arbete idag upplevs vara just det som i rapporten anges ska undvikas – spretigt och svårhanterligt. Utifrån hur Stadens IT-miljö är uppbyggd är dataskyddsombudets bedömning att det i många fall krävs en central styrning för att säkerställa att utvecklingen av AI-lösningar ligger i linje med gällande regelverk. Dataskyddsombudet ser även att det bör ligga i kommunstyrelsens intresse att mer styrning kommer på plats, både för att kunna hantera de brister som identifierats och motverka att de uppstår igen.

Under hösten har dataskyddsombudet och dataskyddsfunktionen haft dialog i flera AI-relaterade frågor, och dataskyddsombudets uppfattning är att de båda enheterna har haft samsyn kring behovet av ökad central styrning. I början av december månad fick dataskyddsombudet information från den nya dataskyddsfunktionen vid stadsledningskontoret att man även därifrån lyft behovet av stadengemensamma AI-regler. Som en konsekvens av detta bildades i mitten av december en arbetsgrupp bestående av dataskyddsfunktionen tillsammans med stadsjuridiska med uppdraget att ta fram ett styrande och vägledande dokument som ska komplettera den allmänna information om AI som idag finns tillgänglig via intranätet.

Dataskyddsombudet är mycket positiv till att man inom förvaltningen reviderat den bedömning som gjordes under arbetet med budgetuppdraget kopplat till behov av central styrning, och att förvaltningen nu i stället aktivt arbetar för att stärka den centrala styrningen i AI-frågor. Utifrån det behov av ökad central vägledning och styrning som bedöms finnas inom Stadens verksamheter när det gäller AI-frågor rekommenderas förvaltningen att under 2025 prioritera arbetet med frågan.

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:

- Vidta åtgärder för att säkerställa att medarbetare informeras om att det är ett lagkrav att involvera dataskyddsombudet i alla frågor som gäller dataskydd.
- Genomför riktade utbildningsinsatser inom förvaltningen med syftet att stärka den allmänna kunskapsnivån (i dataskydd) inom verksamheten.

- Ta fram interna dokumenterade arbetssätt som tydliggör när och hur dataskyddsombudet ska involveras i förvaltningens arbete.

Kommentarer och rekommendationer:

Uppföljningen visar att stadsledningskontoret under hösten 2024 har genomfört en obligatorisk utbildningsinsats i dataskydd för samtliga medarbetare. Syftet med utbildningen har varit att stärka den allmänna kunskapsnivån i dataskydd, i linje med dataskyddsombudets rekommendationer. Inom ramen för utbildningen har medarbetare även fått information om dataskyddsombudets roll och förvaltningens skyldighet att involvera dataskyddsombudet i alla frågor som gäller dataskydd. Under året har även CISO vid stadsledningskontoret tillhandahållit en stadengemensam utbildning i informationssäkerhet, inom vilken ett avsnitt om dataskydd ingår.

När det gäller rekommendationen att ta fram interna dokumenterade arbetssätt för när och hur dataskyddsombudet ska involveras i förvaltningens arbete anger förvaltningen att man under året infört en ny rutin för att säkerställa att alla tröskelanalyser stäms av med dataskyddsombudet. Förvaltningen anger även att det pågår ett arbete med att kartlägga processer och ta fram rutiner för flera olika delar av dataskyddsarbetet, och att det då ingår hur dataskyddsombudet ska involveras i de olika processerna. När förslag på rutiner finns framtagna kommer dessa att stämmas av med dataskyddsombudet, och när rutinerna färdigställts kommer medarbetare inom förvaltningen att informeras om dessa.

Av uppföljningen framgår att förvaltningen under året arbetat aktivt med att omhänderta de rekommendationer som lämnades 2023. Det är mycket positivt att förvaltningen genomfört en obligatorisk utbildning i dataskydd och inom ramen för den lyft dataskyddsombudets roll. Förhoppningsvis bidrar utbildningsinsatsen till att stärka den allmänna kunskapsnivån inom förvaltningen som helhet. Förvaltningen har vid avstämning med dataskyddsombudet uppgett att medarbetare inom olika verksamhetsgrenar efter utbildningen kontaktat dataskydds-organisationen med frågor kopplat till dataskydd, vilket är en indikation på att utbildningen ökat medvetenheten inom förvaltningen. Det är nu viktigt att den interna dataskyddsorganisationen fortsätter att lyfta dataskyddsfrågor och startar upp arbete med de verksamhetsgrenar som hittills inte arbetat aktivt med dataskydd.

Förvaltningen behöver även fortsätta med arbetet att kartlägga processer och ta fram rutiner för när och hur dataskyddsombudet ska involveras. Då dataskyddsombudet fortfarande upplever att förvaltningen inte involverar dataskyddsombudet i tillräcklig utsträckning rekommenderas förvaltningen att prioritera detta arbete under 2025.

Under 2025 kommer dataskyddsombudet löpande följa upp förvaltningens arbete med att ta fram dokumenterade arbetssätt. Dataskyddsombudet kommer även utvärdera ifall utbildningsinsatsen fått effekt genom att mäta om antalet frågor dataskyddsombudet involveras i under 2025 ökar jämfört med tidigare år.

Fokusområde 2: Biträdesavtal och andra överenskommelser

Verksamheten gavs följande rekommendationer:

- Ta ansvar för att driva frågan om att utreda ansvarsförhållanden för staden gemensamma personuppgiftsbehandlingar.

Kommentarer och rekommendationer:

I uppföljningen anger förvaltningen fyra åtgärder som genomförts under året. Dessa aktiviteter är; 1) att förvaltningen genomfört ett arbete tillsammans med förvaltningen för Intraservice för att identifiera vem som är personuppgiftsansvarig för gemensamma system, 2) att förvaltningen ingått i en grupp som startades av direktörer/VD:ar efter en s.k. Bulls Eye-övning och som har arbetat med frågor kopplat till informationssäkerhet och dataskydd, 3) att förvaltningen under våren genomförde en rättsutredning av fördelning av personuppgiftsansvar för en av kommunfullmäktige beslutad migrering av Framtidenkoncernens bolag till Intraservices IT-miljö samt 4) att dataskyddsfunktionen som inrättades under hösten har börjat utreda om det är möjligt att förtydliga personuppgiftsansvaret i staden.

Av de åtgärder som förvaltningen anges ha vidtagits för att hantera rekommendationen är dataskyddsombudets bedömning att enbart den genomförda rättsutredningen och att dataskyddsfunktionen påbörjat ett arbete i frågan kan anses vara initierade av stadsledningskontoret. Dataskyddsombudet har deltagit i både den utredning som genomförts, och pådrivits, av Intraservice samt i det andra arbete som hänvisas till. I båda dessa fall har Intraservice haft en ledande roll och tagit på sig ansvar för att, i samverkan med dataskyddsombudet, driva frågan om ansvarsförhållanden. Stadsledningskontorets roll i det arbetet har varit begränsad och främst handlat om förankring av de bedömningar som Intraservice och dataskyddsombudet gjort.

Utifrån ovan är dataskyddsombudets bedömning att stadsledningskontoret under året inte tagit sitt ansvar för att driva frågan om utredning av ansvarsförhållanden i den utsträckning som borde ha gjorts. Dataskyddsombudets rekommendation har även vid dialog med representanter från stadsledningskontoret ifrågasatts med hänvisning till att man från förvaltningens sida inte förstår varför det är viktigt att utreda ansvarsfördelningen. Då ett utrett personuppgiftsansvar är en grundläggande förutsättning för att Stadens verksamheter ska kunna hantera sina skyldigheter enligt dataskyddsförordningen ser dataskyddsombudet anledning att anmärka på förvaltningens tidigare ingång i frågan.

Under slutet av 2024 har dataskyddsombudet haft möten med dataskydds-funktionen och stadsjuridiska gällande arbetet med att utreda ansvarsförhållanden. Förvaltningen har vid dessa möten angett att man avser prioritera arbetet med frågan under 2025, vilket är positivt. Dataskyddsombudet kommer ha en rådgivande roll i arbetet och kommer inom ramen för denna löpande följa upp hur arbetet framskrider. Ny uppföljning kommer göras under hösten 2025.

Fokusområde 3: Register över personuppgiftsbehandlingar

Verksamheten gavs följande rekommendationer:

- Fortsätt det påbörjade arbetet med att inom verksamheten identifiera de interna personuppgiftsbehandlingar som ligger inom kommunstyrelsens ansvar.

Kommentarer och rekommendationer:

Förvaltningen anger i uppföljningen att det under året har upphandlats ett nytt system/it-stöd för bland annat register över personuppgiftsbehandlingar av förvaltningen för Intraservice och att detta nu håller på att införas. Kopplat till det nya systemet har dataskyddsfunktionen påbörjat ett arbete med att identifiera personuppgiftsbehandlingar inom verksamhetsområde 1 och 2 enligt klassificeringsstrukturen, vilka är gemensamma för alla förvaltningar och bolag. Förvaltningen inväntar nu det arbetet och när behandlingar inom dessa verksamhetsområdena identifierats är tanken att stadsledningskontorets interna arbete med att identifiera och dokumentera de personuppgiftsbehandlingar som finns inom förvaltningens övriga verksamhetsområden ska fortsätta.

Dataskyddsombudet är mycket positiv till att stadsledningskontoret nu, genom dataskyddsfunktionen, tar ett helhetsgrepp i frågan om identifiering och ansvarsbedömning av gemensamma personuppgiftsbehandlingar (inom verksamhetsområde 1 och 2). I detta arbete har dataskyddsfunktionen och dataskyddsombudet ett nära samarbete, eftersom resultatet är tänkt att kunna användas av alla förvaltningar och bolag i Staden. För att arbetet ska få önskad effekt är det viktigt att man i arbetet utgår från de krav som ställs enligt dataskyddslagstiftningen och inte kompromissar med dessa, även om kraven innebär ett initialt ökat administrativt arbete för verksamheter. Dataskyddsombudet är övertygad om att ett korrekt utformat register över personuppgiftsbehandlingar kommer bidra till att underlätta dataskyddsarbetet inom förvaltningar och bolag, och därigenom minska administrationen i flera andra dataskyddsfrågor. Utifrån detta vill dataskyddsombudet särskilt betona vikten av att det förslag till register som nu tas fram motsvarar de krav som ställs i artikel 30 GDPR.

När det gäller stadsledningskontorets register över de personuppgiftsbehandlingar som ligger inom kommunstyrelsens ansvar rekommenderade dataskyddsombudet i årsrapporten 2023 förvaltningen att prioritera det arbetet. Denna rekommendation kvarstår för 2025 och förvaltningens interna dataskyddsorganisation rekommenderas arbeta med frågan parallellt med det arbete som dataskyddsfunktionen ansvarar för. Dataskyddsombudet kommer under 2025 ha regelbundna avstämningsmöten med förvaltningens dataskyddskontakter och avser vid dessa följa upp hur arbetet med det interna behandlingsregistret fortskrider.

Under 2025 kommer uppföljningen av rekommendationen delas upp i två olika delar. En del kommer att fokusera på dataskyddsfunktionens arbete med det stadengemensamma registret, och en del kommer fokusera på den interna dataskyddsorganisationens arbete med den del av behandlingsregistret som avser behandlingar inom kommunstyrelsens ansvar.

5 Rekommenderade fokusområden 2025

Dataskyddsombudet rekommenderar, utifrån gjorda iakttagelser och resultaten av uppföljningen, verksamheten att under 2025 fortsätta prioritera arbetet med de kontrollpunkter som rekommenderas för 2024. Dessa 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

Inom ramen för denna kontrollpunkt inkluderas rekommenderade åtgärder för att hantera de risker som identifierats under avsnitt 3.1, 3.2 och 4.2.

1) Ta fram interna dokumenterade arbetssätt som tydliggör när och hur dataskyddsombudet ska involveras i förvaltningens arbete.

Inom ramen för arbetet med att kartlägga processer och ta fram rutiner för hur dataskyddsombudet ska involveras i de olika processerna rekommenderas förvaltningen prioritera hur dataskyddsombudet ska involveras i den interna ärendeberedningen samt i förvaltningens arbete med digitalisering och innovation.

2) Prioritera arbetet med att ta fram en central vägledning/styrning i AI-frågor för Stadens verksamheter.

- Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Ta ansvar för att driva frågan om att utreda ansvarsförhållanden för stadengemensamma personuppgiftsbehandlingar.

- Kontrollpunkt 4: Register över personuppgiftsbehandlingar

1) Fortsätt arbetet med att identifiera och bedöma ansvarsförhållanden för de personuppgiftsbehandlingar som finns inom verksamhetsområde 1 och 2, och är gemensamma för Stadens förvaltningar och bolag.

2) Fortsätt arbetet med att identifiera de personuppgiftsbehandlingar som ligger inom kommunstyrelsens ansvar och dokumentera de identifierade behandlingarna i behandlingsregistret.

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

6 Bilagor

Bilaga 1: Kontrollplan för dataskyddsarbetet 2024–2025