Göteborgs Stad

Årsrapport för dataskyddsarbetet 2024

Nämnden för inköp och upphandling

2024-12-19

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 arbetat nära förvaltningens dataskyddskontakt och blivit involverad i de dataskyddsfrågor som aktualiserats. Samarbetet mellan dataskyddsombudet och förvaltningen upplevs fungera bra och förvaltningens dataskyddsarbete bedöms ha stärkts under året. Att förvaltningen under året även resurssatt inom informationssäkerhetsområdet är positivt eftersom det ger goda förutsättningar i dataskyddsarbetet framåt. Dataskyddsombudets uppfattning är att det inom förvaltningen finns en god ambitionsnivå och vilja att börja arbeta med dessa frågor mer systematiskt.

Under året har förvaltningen bland annat arbetat med frågor kopplat till reglering av ansvarsförhållanden med verksamheter inom Staden, hanteringen av personuppgiftsbiträdesavtal vid tecknande av RAM-avtal, leverantörsrelationer och behandling av personuppgifts i samband med bakgrundskontroller. Förvaltningen har även genomfört ett antal konsekvensbedömningar och tröskelanalyser vilka varit väl genomförda och hållit en bra kvalitet.

3.2 Särskilda iakttagelser

3.2.1 Förvaltningen bidrar till att stärka Stadens dataskyddsarbete som helhet

Förvaltningens arbete med en ny tjänst för hantering av upphandling, avtal och leverantörer (ULA) har pågått under flera år. Dataskyddsombudet har under tiden arbetet pågått löpande lämnat rekommendationer i olika dataskyddsfrågor. Under 2024 genomförde förvaltningen ett omfattande dataskyddsarbete inför piloten av ULA. Inom ramen för detta kartlades och bedömdes ansvarsförhållanden för de personuppgiftsbehandlingar som aktualiseras vid användning av tjänsten, samtidigt som information till registrerade togs fram och en konsekvensbedömning genomfördes. Det ansvar som förvaltningen tog inför införandet av ULA ligger i linje med förvaltningens ansvar som intern tjänsteleverantör, och gynnar såväl den egna verksamheten som övriga förvaltningar och bolag i Staden.

Då det är första gången en intern tjänsteleverantör arbetar på det här sättet och tar ansvar för stadengemensamma dataskyddsfrågor vill dataskyddsombudet särskilt uppmärksamma nämnden på förvaltningens arbete. Utöver att förvaltningens arbete underlättar för andra verksamheter i Staden inför att de ska börja använda systemet, bidrar det även till att stärka skyddet för de registrerade och underlätta hanteringen av de registrerades rättigheter. Sammantaget bedöms förvaltningen genom dess arbete ha bidragit till att stärka Stadens dataskyddsarbete som helhet.

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 7: 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.

Kommentarer och rekommendationer:

Uppföljningen visar att förvaltningen under året har arbetat med informationsplikten på olika sätt. Bland annat har ett omfattande arbete gjorts inom ramen för ULA-projektet då man tagit fram en fördjupad information om hantering av personuppgifter till de som vill bli leverantörer till Göteborgs stad.

Förvaltningen har under året också fokuserat på kundrelationer och den del av verksamheten som berör event och utbildningar. I dessa delar har förvaltningen arbetat med att säkerställa att tillhandahålla en länk till förvaltningens informationspolicy i samband med utbildningar, nätverk och inbjudningar samt i anställdas mejlsignaturer. Under 2025 planeras även en riktad utbildningsinsats för den avdelning inom förvaltningen som ansvarar för kundrelationer samt event och utbildningar.

Det är positivt att förvaltningen arbetat med frågan. Då informationsplikten gäller för alla behandlingar är det en fråga som förvaltningen kommer behöva fortsätta att arbeta med. En förutsättning för att förvaltningen ska kunna uppfylla kraven på vilken information som lämnas är att behandlingsregistret är fullständigt och att ansvarsfördelningen för olika personuppgiftsbehandlingar är utredda. För att få in en systematik i arbetet med informationsplikten rekommenderas förvaltningen att se över och kartlägga hur information ges om de olika behandlingarna idag, och utifrån det göra upp en planering för det vidare arbetet.

Fokusområde 10: IT-projekt och upphandling

Verksamheten gavs följande rekommendationer:

- Kartlägga kompetensbrister och tillhandahålla utbildning.

Kommentarer och rekommendationer:

Uppföljningen visar att förvaltningen under året har arbetet aktivt med att omhänderta rekommendationerna. Förvaltningen har påbörjat en större kartläggning av gemensamma avtal för att identifiera var det föreligger störst risk och/eller behov kopplat till informationssäkerhet och dataskydd. Utifrån denna kartläggning kommer också kompetensbehovet kartläggas, så att insatserna riktas dit behoven är som störst. Målet är att arbetet ska resultera i en systematik där informationssäkerhet och dataskydd omhändertas tidigt i processen och integreras i arbetet med avtalsstrategi.

Dataskyddsombudet bedömer det positivt att förvaltningen nu tagit ett helhetsgrepp i frågan och rekommenderar förvaltningen att fortsätta prioritera arbetet under 2025.

Fokusområde 11: IT-system och digitala verktyg

Verksamheten gavs följande rekommendationer:

- Ta fram förvaltningsövergripande arbetssätt/rutiner för tilldelning och uppföljning av behörigheter och åtkomster i IT-system som tar

utgångspunkt i det som medarbetarna behöver ha tillgång till för att utföra sina arbetsuppgifter.

Kommentarer och rekommendationer:

Uppföljningen visar att förvaltningen arbetat med behörighetsstyrning inom ramen för ULA-projektet och införandet av ett nytt system. När det gäller övriga IT-system och digitala verktyg anger förvaltningen att man under hösten har resursförstärkt inom både IT/digitalisering och informationssäkerhet och att arbetet med behörighetsstyrning kommer att byggas upp under 2025.

Utifrån att förvaltningen under 2024 inte arbetat med frågan, utöver inom ramen för ULA-projektet, behöver förvaltningen under 2025 fortsätta arbetet med att omhänderta rekommendationerna.

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 7: Informationsplikt

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.

- Kontrollpunkt 10: IT-projekt och upphandling

Kartlägga kompetensbrister och tillhandahålla utbildning.

- Kontrollpunkt 11: IT-system och digitala verktyg

Ta fram förvaltningsövergripande arbetssätt/rutiner för tilldelning och uppföljning av behörigheter och åtkomster i IT-system som tar utgångspunkt i det som medarbetarna behöver ha tillgång till för att utföra sina arbetsuppgifter.

6 Bilagor

Bilaga 1: Kontrollplan för dataskyddsarbetet 2024–2025