Göteborgs Stad

Årsrapport för dataskyddsarbetet 2024

Stadsmiljönämnden

2024-12-17

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 kvarstår vid tidigare års bedömning om att förvaltningen har en organisation för sitt dataskyddsarbete med mycket hög kompetens hos förvaltningens interna dataskyddsorganisation. Förvaltningen har kommit långt i sitt systematiska dataskyddsarbete, framför allt i arbetet med att genomföra konsekvensbedömningar för de behandlingar som bedöms innebära höga risker för de registrerade. I likhet med många andra verksamheter i Staden, behöver dock dataskyddsfrågorna få ett tydligare genomslag i organisationen som helhet. Det är också viktigt att förvaltningens dataskyddskontakter involveras i ett tidigt skede i samtliga frågor som rör dataskydd, i enlighet med vad som framgår av verksamhetens dokumenterade arbetssätt.

Dataskyddsombudet har under året gjort en särskild genomgång av förvaltningens dataskyddsorganisation och de dokumenterade arbetssätt och roll- och ansvarsbeskrivningar som finns på plats inom dataskyddsområdet. Med ledning av detta har dataskyddsombudet lämnat ett antal råd till förvaltningen om hur roller och ansvar kan tydliggöras för att säkerställa ett än mer funktionellt dataskyddsarbete. Dataskyddsombudets bedömning är att förvaltningen tagit till sig dessa råd och börjat implementera dem.

4 Granskning av dataskyddsarbetet 2024

4.1 Fördjupad kontroll 2024

Dataskyddsombudet genomförde under hösten 2024 en fördjupad kontroll av stadsmiljöförvaltningens register över personuppgiftsbehandlingar i enlighet med artikel 30 i GDPR. Enligt artikel 5.2 i GDPR är det den personuppgiftsansvarige som ansvarar för och ska kunna visa att organisationen följer GDPR och efterlever de grundläggande principerna i artikel 5.1 i GDPR. Som ett led i ansvarsskyldigheten följer det av artikel 30.1 och skäl 82 i GDPR och att den personuppgiftsansvarige ska föra ett register över sina behandlingar. Det framgår vidare av artikel 30.3 att registret ska vara skriftligt, och av artikel 30.4 att registret på begäran ska göras tillgängligt för tillsynsmyndigheten.

Dataskyddsombudets sammanfattande bedömning av dom organisatoriska förutsättningarna för att förvaltningen ska kunna uppfylla kraven i artikel 30 i GDPR, är att verksamheten till stor del har dokumenterade arbetssätt på plats, men att det tydligare behöver framgå vem som internt ansvarar för att registret uppfyller kraven i GDPR. Förvaltningen rekommenderas också att förtydliga de enskilda kontaktpersonernas ansvar och hur dessa utses.

Vad gäller granskningen av själva behandlingsregistret framgår att förvaltningen anser att det register som tillhandahållits dataskyddsombudet innehåller komplett information i enlighet med kraven i artikel 30 i GDPR. Dataskyddsombudets samlade bedömning är att registret endast delvis innehåller den information som föreskrivs enligt artikel 30 och att de uppgifter som finns dokumenterade i registret har stora brister. Dataskyddsombudet rekommenderar därför att förvaltningen tar ett omtag kring: hur verksamheten dokumenterar sina behandlingar i behandlingsregistret, särskilt med fokus på att formulera tydliga, konkreta och specifika ändamål, hur man beskriver de kategorier av personuppgifter och kategorier av registrerade som förekommer i de olika behandlingarna, vilka som är mottagare av uppgifterna, tidsfrister för radering av personuppgifter och en allmän beskrivning av skyddsåtgärder. Dataskyddsombudet redogör i detalj för sin bedömning i rapporten för den fördjupade kontrollen, se bilaga 2.

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. Utifrån uppföljningen lämnas rekommendationer.

Fokusområde 1: IT-projekt och upphandling

Verksamheten gavs följande rekommendationer:

- Ta ett omtag kring upphandlingen av nytt system för reseplanering så att processen följer de dokumenterade arbetssätt som finns inom förvaltningen för hur upphandlingar ska genomföras och tillse att principerna om inbyggt dataskydd, och dataskydd som standard beaktas.

- Säkerställ att dokumenterade arbetssätt för hur upphandlingar ska genomföras efterlevs, och anta interna riktlinjer för att hantera situationer där internt beslutade arbetssätt inte efterlevs.

Kommentarer och rekommendationer:

Som svar på dataskyddsombudet uppföljning uppger förvaltningen att avdelning Serviceresor och mobilitet har fortsatt med den påbörjade upphandlingen. Ansvarig verksamhet omformulerade upphandlingsunderlaget i fas 1, för att förtydliga att förvaltningen söker en helhetslösning för de system som ska upphandlas. Dataskyddsperspektivet har diskuterats med dataskyddsombudet och den interna dataskyddsfunktionen på gemensamt möte. En preliminär konsekvensbedömning har genomförts där både dataskyddsombudet och den interna dataskyddsfunktionen på förvaltningen lämnat synpunkter och råd/rekommendationer kring vad som är viktigt att säkerställa i senare delar av upphandlingen.

Upphandlingen är inte slutförd än, det betyder att val av leverantör och lösning inte har gjorts. Inför att nytt system tas i bruk kommer konsekvensbedömning behöva göras i en ny version för att säkerställa att val av leverantör, lösning och andra faktorer som inte var känt när den preliminära konsekvensbedömningen gjordes, inte leder till höga risker. Detta kommer hanteras enligt gängse rutiner. En informationsklassning har genomförts och med detta som underlag har en kravspecifikation tagits fram för att säkerställa nödvändiga tekniska och organisatoriska säkerhetsåtgärder hos leverantör. Den interna dataskyddsfunktionen deltar i relevanta delar av upphandlingen. Dataskyddsombudet kommer att involveras i arbetet med konsekvensbedömningen.

Visst arbete med att förtydliga delegationsordningen har gjorts, så att det nu är tydligt när/under vilka förutsättningar en avdelningschef kan fatta beslut om att godkänna en personuppgiftsbehandling och när det enbart är möjligt att gå till

förhandsamråd alternativt inte påbörja behandlingen. I övrigt pågår diskussion/arbete med att se över frågan om rutiner för detta.

Dataskyddsombudet anser att förvaltningen omhändertagit rekommendationerna som lämnades och att någon särskild uppföljning inte behöver ske under 2025 med mer än att dataskyddsombudet involveras i den mån som krävs avseende arbetet med konsekvensbedömning av de behandlingar som ska utföras i systemet.

Fokusområde 2: IT-system och digitala verktyg

Verksamheten gavs följande rekommendationer:

- Förvaltningen rekommenderas att upprätta konsekvensbedömningar för de behandlingar där kameror används som innebär höga risker för de registrerade.

- Utred och få klarhet i frågan om de rättsliga förutsättningarna för delning av kameraströmmar till externa aktörer, till exempel inom samarbetet för Trafik Göteborg.

Kommentarer och rekommendationer:

Som svar på dataskyddsombudets uppföljning uppger förvaltningen att man har tagit fram en konsekvensbedömning för det interna bruket av trafikkameror och att den är färdigställd. Konsekvensbedömning för spårvägskameror är också slutförd. Arbete med konsekvensbedömning för extern delning och anläggningskameror pågår också, men denna är beroende av pågående utredning av ansvarsfrågan.

Förvaltningen har tecknat ett avtal med räddningstjänsten avseende deras nyttjande av videoströmmar, där har förvaltningen bedömt att det inte finns något gemensamt personuppgiftsansvar. Förvaltningen har utrett delningen inom Trafik Göteborg och de rättsliga förutsättningarna för denna. Trafikverket agerar där som personuppgiftsbiträde åt stadsmiljöförvaltningen. Arbetet med att uppdatera samarbetsavtal och skriva personuppgiftsbiträdesavtal pågår. Delningen till Västtrafik utreds fortfarande tillsammans med Västtrafik och förvaltningen kommer så snart som möjligt slutföra den utredningen. Förvaltningen har också kameror där Parkeringsbolaget är personuppgiftsbiträde, för detta finns personuppgiftsbiträdesavtal. Förvaltningen delar inte längre kameraströmmar till exploateringsförvaltningen. Inför framtida eventuella delningar kommer förvaltningen utreda de rättsliga förutsättningarna och teckna nödvändiga avtal innan delning påbörjas.

Dataskyddsombudets bedömning är att förvaltningen har tagit stora steg för att omhänderta de rekommendationer som lämnats, även om delar av rekommendationerna kvarstår, och bedömer att ingen särskild uppföljning krävs, utan att kontrollpunkten kan följas upp inom ramen för ordinarie avstämningar med verksamheten

5 Rekommenderade fokusområden 2025

Dataskyddsombudet har under arbetet med årsrapporten identifierat ett område som verksamheten rekommenderas att särskilt arbeta med under det kommande året.

Detta är ett område 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 under 2025 prioritera följande delar av dataskyddsarbetet:

- Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Dataskyddsombudet genomförde under hösten 2024 en fördjupad kontroll av förvaltningens arbete med behandlingsregister enligt artikel 30 i GDPR (se även fördjupad kontroll). Kontrollen visade på brister i förvaltningens dokumentation av behandlingar i sitt behandlingsregister. Förvaltningen rekommenderas därför att fokusera på att omhänderta de rekommendationer som dataskyddsombudet lämnat i rapporten för den fördjupade kontrollen.

6 Bilagor

Bilaga 1: Kontrollplan för dataskyddsarbetet 2024–2025

Bilaga 2: Fördjupad kontroll 2024