Göteborgs Stad

Årsrapport för dataskyddsarbetet 2024

Higab AB

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 haft en aktivt rådgivande roll i arbetet att genomföra delar av bolagets arbete under 2024. Dataskyddsombudet har involverats i avstämningsmöten och konsulterats av verksamheten i frågor rörande dataskydd hänförliga till såväl granskning som förvaltning bland andra i arbetet med tröskelanalyser och konsekvensbedömningar. Dataskyddsombudet uppfattning är att det finns ett stort intresse för frågor om integritet och dataskydd vilket är positivt och en viktig förutsättning för bolagets fortsatta utveckling. Det är också viktigt att bolagsledningen fortsätter att tydligt prioritera frågor kopplat till integritet och dataskydd.

Det finns fortfarande utmaningar för bolaget att utveckla sitt dataskyddsarbete. Avgörande för att bli framgångsrik i detta är ett långsiktigt och uthålligt engagemang för att bedriva arbetet kontinuerligt. Eftersom arbetet berör hela verksamheten är det viktigt att alla medarbetare är medvetna om detta. God nivå i dataskyddsarbetet byggs genom kunskap underifrån och stöd av strukturer och arbetssätt för varje verksamhet.

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. Utifrån uppföljningen lämnas rekommendationer.

Fokusområde 1: Biträdesavtal och andra överenskommelser

Verksamheten gavs följande rekommendationer:

Verksamheten rekommenderas ta fram dokumenterade arbetssätt för att bedöma ansvarsfördelning när en leverantör anlitas som innefattar bedömning och efterlevnadskontroller av anlitade biträden samt hela kedjan av underbiträden.

Kommentarer och rekommendationer:

Av uppföljningen framgår att bolagets inventering av samtliga biträdesrelationer är klar. Biträdesavtal i enlighet med GDPR kraven finns med alla utom tre leverantörer. Bolagets bedömning är att avsaknad av biträdesavtal inte är av akut karaktär då relation med en av leverantörerna ändå håller på att fasas ut och när det gäller de två övriga behandlas endast fastighetsbeteckning samt medarbetarnas namn och mejluppgifter.

Dataskyddsombudet har inte tagit del av bolagets ansvarsfördelningsbedömning och har inte heller någon anledning att ifrågasätta om den är korrekt.

Uppgift huruvida dokumenterade arbetssätt har tagits fram parallellt med inventeringsarbetet framgår inte tydligt och är så inte fallet kvarstår rekommendationen i den delen.

Fortsatt uppföljning kommer därför att ske löpande under ordinarie avstämningsmöten eller inom ramen för den uppföljning som dataskyddsombudet genomför under hösten 2025.

Fokusområde 2: Utbildning

Verksamheten gavs följande rekommendationer:

Verksamheten rekommenderas kartlägga behov av olika typer av utbildningsinsatser, se till att de genomförs, följs upp samt dokumenteras.

Kommentarer och rekommendationer:

Enligt uppgift har bolaget fått tillgång till utbildningar i stadens Utbildningsportal och därmed också till bland andra den obligatoriska digitala utbildningen i GDPR samt informationssäkerhet. Detta innebär också att bolaget kan lägga upp egna utbildningsinsatser och att både uppföljning och dokumentation underlättas därmed. Bolaget uppger också att GDPR informationen har lagts in i nyintroduktionsblocket.

Uppföljningen visar att verksamheten har vidtagit åtgärder i enlighet med samtliga rekommendationer. Fortsatt uppföljning kommer att ske löpande under ordinarie avstämningsmöten eller inom ramen för den uppföljning som dataskyddsombudet genomför under hösten 2025.

Fokusområde 3: Hantering av registrerades rättigheter

Verksamheten gavs följande rekommendationer:

Verksamheten rekommenderas att öka medarbetarnas kunskap om de registrerades rättigheter samt ha beredskap och dokumenterat arbetssätt för att hantera begränsning och ett tillbakadragande av ett samtycke.

Kommentarer och rekommendationer:

Som svar på dataskyddsombudets uppföljningsfrågor har bolaget uppgett att de upplever att verksamhetens kontroll och kunskaper kring GDPR frågor generellt har blivit bättre genom olika utbildningsinsatser.

Enligt uppgift har bolaget inte fått frågan om att hantera begräsning och inte heller tillbakadragande av ett samtycke. När det gäller samtycke som rättslig grund uppger bolaget att beredskapen ändå finns genom att en översyn av bildtagning har gjorts och att även samtyckesblanketten för medarbetare har kompletterats upp med angivande av exakta marknadsföringsåtgärder och insatser när en bild används. Vidare uppges bolaget ha gjort ett medvetet val att inte använda kunder eller leverantörer på bild som en *generell* marknadsföringsinsats utan alltid som en illustration med en direkt koppling till exempelvis en artikel.

Av uppföljningssvaren framgår också att ur ett GDPR-perspektiv rekommenderas verksamheten att använda Stadens bildbank vilket den interna dataskyddsorganisationen i bolaget instämmer i och har också framfört till ansvariga.

Dataskyddsombudets samlade bedömning är att bolaget aktivt arbetat med frågan och rekommenderas fortsätta på den inslagna linjen. Fortsatt uppföljning kommer därför att ske löpande under ordinarie avstämningsmöten eller på förekommen anledning.

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 med tilläggsfokus som 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.

Bolaget rekommenderas under 2025 prioritera följande delar av dataskyddsarbetet:

- Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Kartlägga och dokumentera personuppgiftsbehandlingar enligt artikel 30 i GDPR. Ta del av den generella granskningsrapporten från dataskyddsombudets fördjupade kontroll och beakta rekommendationerna som framgår däri vid arbete med behandlingsregistret.

- Kontrollpunkt 9: Konsekvensbedömningar/samråd

Inhämta dataskyddsombudets synpunkter för pågående liksom framtida konsekvensbedömningar. Säkerställa förbättringsåtgärderna och inkorporera ett arbetssätt för att och i de fall där så krävs även inhämta de registrerades synpunkter.

6 Bilagor

Bilaga 1: Kontrollplan för dataskyddsarbetet 2024–2025