Göteborgs Stad

Årsrapport för dataskyddsarbetet 2024

Bostads AB Poseidon

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

Kontakten mellan dataskyddsombudet och bolaget har under året främst utgjorts av deltagande vid Framtidenskoncernens gruppmöten inom dataskydd och då bolaget har tagit kontakt vid verksamhetsspecifika frågor, personuppgiftsincidenter och i samband med en konsekvensbedömning. Dataskyddsombudet finner det som positivt att dataskyddsombudet involveras och uppmuntrar bolaget att även framåt ta kontakt med dataskyddsombudet vid frågor som rör dataskydd. Samtidigt ser dataskyddsombudet, utifrån verksamhetens karaktär, ett behov av mer regelbunden kontakt för att säkerställa att bolaget uppfyller kravet enligt artikel 38.1 i GDPR gällande att dataskyddsombudet ska involveras i alla frågor som gäller dataskydd.

Även om bolaget ges rekommendationer i förhållande till andra kontrollpunkter i uppföljningen, är dataskyddsombudets rekommendation att bolaget under 2025 särskilt fokuserar på de fokusområden som framgår av avsnitt 5. Att regelbundet involvera dataskyddsombudet och att ha ett uppdaterat register över bolagets personuppgiftsbehandlingar utgör ett led i att bedriva ett systematiskt dataskyddarbete. Det kommer också, enligt dataskyddsombudet, ge bättre förutsättningar för bolaget att arbeta med övriga delar av dataskyddsarbetet.

4 Granskning av dataskyddsarbetet 2024

4.1 Fördjupad kontroll 2024

Dataskyddsombudet genomförde under hösten 2024 en fördjupad kontroll av bolagets 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 samlade bedömning är att bolaget behöver se över hur behandlingarna är definierade och avgränsade i behandlingsregistret då det bedöms finnas ett behov av att bryta ner flera av behandlingarna i mindre delar.

Vidare är dataskyddsombudets bedömning att behandlingsregistret delvis innehåller den information som föreskrivs enligt art. 30 i GDPR och anser att det finns delar som behöver kompletteras eller förtydligas. Dataskyddsombudet anser, i ett första steg, att ett särskilt fokus behöver läggas på att formulera tydliga, konkreta och specifika ändamål. Även beskrivning av de kategorier av personuppgifter och kategorier av registrerade som förekommer i de olika behandlingarna, tidsfrister för radering av personuppgifter och en allmän beskrivning av organisatoriska säkerhetsåtgärder behöver kompletteras.

Dataskyddsombudet rekommenderar även att bolaget upprättar dokumenterade arbetssätt för hantering av behandlingsregistret internt samt att dessa fastställs officiellt genom beslut. I detta ingår att fastställa tydligt utpekade roller och ansvar för att löpande hålla behandlingsregistret uppdaterat och i enlighet med lagkraven. För samtliga rekommendationer, se granskningsrapporten 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: Konsekvensbedömningar/samråd

Verksamheten gavs följande rekommendationer:

- Bedöm befintliga personuppgiftsbehandlingar utifrån höga risker för att få en överblick över vilka av personuppgiftsbehandlingarna som kräver en konsekvensbedömning. Ta fram en långsiktig planering för att genomföra konsekvensbedömningar.

Kommentarer och rekommendationer:

Verksamheten uppger under uppföljningen att det har gjorts en översyn av samtliga behandlingar. Verksamheten har ett excel-ark med samtliga bolagets personuppgiftsbehandlingar specificerade utifrån behandlingsregistret. Utifrån excel-arket har bolaget markerat vilka behandlingar som bedömas behöva en konsekvensbedömning. I samband med arbetet har en prioritering och planering gjorts. Planeringen är framtagen utifrån en bedömning av resurser och inom vilken tidsaspekt som verksamheten tror att konsekvensbedömningarna är praktiskt genomförbara.

Bolaget har för närvarande en projektanställd informationssäkerhetssamordnare som har påbörjat arbetet med att klassa information och utse informationsägare. Genom att utse olika informationsägare hoppas verksamheten på att ansvaret för konsekvensbedömningar ska kunna spridas ut och att informationsägarna får ett tydligare ansvar över konsekvensbedömningar.

Dataskyddsombudet har inte tagit del av bolagets framtagna planering, men har ingen anledning att ifrågasätta att en sådan tagits fram. Utifrån vad verksamheten uppger under uppföljningsmötet har bolaget omhändertagit dataskyddsombudets rekommendationer. Framåt är det viktigt att bolaget säkerställer att konsekvensbedömningarna även genomförs i praktiken.

Som framgår under avsnitt 4.1. har bolaget varit föremål för den fördjupade kontrollen av behandlingsregistret. Hur en behandling definieras och avgränsas är av betydelse för övriga delar av dataskyddsarbetet, bland annat vid arbetet med konsekvensbedömningar. Bolaget kommer därför att rekommenderas att särskilt arbeta med behandlingsregistret under året för att underlätta arbetet med genomförandet av konsekvensbedömningar framåt.

Fokusområde 2: IT-system och digitala verktyg

Verksamheten gavs följande rekommendationer:

- Se över nuvarande cookiehantering och vidta åtgärder för att säkerställa att användningen av cookies på bolagets webbsida uppfyller kraven enligt såväl dataskyddsförordningen som LEK (lagen (2022:482) om elektronisk kommunikation).

Kommentarer och rekommendationer:

I samband med uppföljningen uppgav verksamheten att det pågick ett arbete med en ny extern leverantör av hemsidan och att lanseringen av hemsidan planerades att ske under november 2024. Vid lanseringen ska cookiehanteringen vara uppdaterad enligt lagkrav.

Dataskyddsombudet hade i början av året en övergripande genomgång av cookie-hantering utifrån Post- och telestyrelsens (PTS) tillsynsbeslut avseende cookies från 2023 med verksamheten. Vid en översiktlig genomgång av bolagets hemsida noterar dataskyddsombudet att cookiehanteringen har uppdaterats, vilket dataskyddsombudet ser som positivt. Dataskyddsombudet ser dock fortsatt att cookiehanteringen behöver förbättras ytterligare. Exempelvis behöver samtliga ändamål med cookies vara tydliga vid insamling av samtycken. Bolaget avråds även från att ha en kategori av cookies som benämnas ”okategoriserad” då dataskyddsombudet är tveksam till om en sådan kategori kan uppfylla kravet på information.

Dataskyddsombudet kommer fortsättningsvis följa bolagets arbete med rekommendationen, men rekommendationen kommer inte att följas upp särskilt i samband med årsrapporten 2025, såvida inget föranleder ett behov av en särskild uppföljning.

Fokusområde 3: Hantering av registrerades rättigheter

Verksamheten gavs följande rekommendationer:

- Se över bolagets rutiner för hantering av registrerades rättigheter och säkerställa att dessa fungerar i praktiken samt är förankrade bland samtliga medarbetare inom bolaget.

Kommentarer och rekommendationer:

Enligt verksamheten finns det etablerade rutiner gällande arbetssätt för registerutdrag och då registrerade önskar utöva sina andra rättigheter. Verksamheten uppger också att dataskyddskontakten har varit ute i verksamheten och informerat medarbetare om registrerades rättigheter många gånger. Alla nyanställda behöver även genomgå en introduktion om dataskyddsförordningen där information om registrerades rättigheter finns med.

Dataskyddsombudet anser att det är positivt att det finns etablerade rutiner för hantering av registrerade rättigheter. Det är dock inte alltid tillräckligt, utan det är också viktigt att säkerställa att medarbetare både har kännedom om rutinerna och förstår vad som förväntas av dem i de fallen registrerade kontaktar bolaget för att utöva sina rättigheter. Utifrån uppföljningen är dataskyddsombudets uppfattning att verksamheten är medvetna om att det krävs ett löpande arbete med att informera medarbetare. Framåt rekommenderas bolaget att fortsätta att arbeta med kunskapshöjande insatser om registrerade rättigheter.

Dataskyddsombudet kommer fortsättningsvis följa bolagets arbete med rekommendationen, men rekommendationen kommer inte att följas upp särskilt i

samband med årsrapporten 2025, såvida inget föranleder ett behov av en särskild uppföljning.

4.2.2 Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförda kontroller

Dataskyddsombudet har under året följt upp vilka åtgärder som vidtagits avseende tidigare års lämnade rekommendationer av gjorda kontroller.

Kontroll (2022): Kamerabevakning

Verksamheten gavs följande rekommendationer:

- Förtydliga bedömningen kring varför bevakningen inte är tillståndspliktig i bolagets underlag.
- Dokumentera bolagets övervägande kopplat till tider som kamerabevakningen sker.
- Se över lagringstiden och dokumentera de överväganden som bolaget gör för att säkerställa att lagringstiden verkligen är befogad i förhållande till ändamålen och omständigheterna kring hur lång tid det tar att upptäcka och hantera en incident.
- Säkerställ att en dokumenterad intresseavvägning finns för samtliga bevakningar.
- Säkerställ att bevakningen på Borgaregatan har ett legitimt ändamål, är nödvändig för att uppnå ändamålet och har en rättslig grund.
- Bedöm om konsekvensbedömningar behöver genomföras utifrån GDPR:s bestämmelser för de bevakningar som det inte har genomförts sådana för.
- Säkerställ att personuppgifterna i inspelat material hanteras på ett tillräckligt säkert sätt.

Kommentarer och rekommendationer:

Verksamheten uppgav i samband med uppföljningen 2023 att verksamheten hade förtydligat i underlaget till varje enskild bevakning varför kamerabevakningen inte är tillståndspliktig. Verksamheten hade även dokumenterat sina överväganden kopplat till tider som kamerabevakning sker samt att överväganden kring lagringstid för bildmaterialet. Verksamheten uppgav även att underlag avseende behovet för kamerabevakning på Borgaregatan hade inhämtats. Bolaget rekommenderades i årsrapporten 2023 att inhämta dataskyddsombudets råd och rekommendationer i dessa delar. Dataskyddsombudet har dock inte tillfrågats under året varför denna rekommendation kvarstår.

Under årets uppföljning uppger verksamheten att det pågår ett arbete med att ta fram en tydlig mall för när exempelvis konsekvensbedömningar ska genomföras. Enligt verksamheten pågår även ett koncerngemensamt arbete för att revidera stödjande anvisningar för kamerabevakning. I samband med uppföljningen 2023 uppgav verksamheten att det pågick ett arbete med en konsekvensbedömning. Under årets uppföljning meddelar verksamheten dock att det inte pågår någon

specifik konsekvensbedömning. Verksamheten uppger att den kamerabevakning som verksamheten bedömer är integritetskänslig är för de kameror som finns uppsatta i Hjällbo. En konsekvensbedömning för kamerabevakning i Hjällbo finns framtagen sedan tidigare.

Om bolaget bedömer att kamerabevakningen på andra platser inte kräver konsekvensbedömningar, rekommenderas bolaget att tydligt motivera varför samt inhämta dataskyddsombudets råd och rekommendationer avseende motiveringarna.

Integritetsskyddsmyndigheten publicerade en uppdaterad vägledning för kamerabevakning 2023. Under det senaste året har det även kommit nya tillsynsbeslut avseende kamerabevakning. Det rekommenderas därför att den framtagna konsekvensbedömningen för kamerabevakningen i Hjällbo ses över inom ramen för det systematiska dataskyddsarbetet. Vid uppdateringar rekommenderas även att dataskyddsombudets råd och rekommendationer inhämtas.

Mot bakgrund av ovan avser dataskyddsombudet att fortsätta följa upp arbetet med kamerabevakningen under 2025.

5 Rekommenderade fokusområden 2025

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

Bolaget rekommenderas under 2025 prioritera följande delar av dataskyddsarbetet:

- Kontrollpunkt 1: Dataskyddsorganisationen:

Säkerställ att dataskyddsombudet involveras mer regelbundet i arbetet med dataskydd, med syftet att säkerställa att bolaget uppfyller kravet enligt artikel 38.1 i GDPR gällande att dataskyddsombudet ska involveras i alla frågor som gäller dataskydd.

- Kontrollpunkt 4: Registret över personuppgiftsbehandlingar:

Ta del av granskningsrapporten från dataskyddsombudets fördjupade kontroll och omhänderta rekommendationerna som framgår av granskningsrapporten.

6 Bilagor

Bilaga 1: Kontrollplan för dataskyddsarbetet 2024–2025

Bilaga 2: Rapport fördjupad kontroll 2024