**Tjänsteutlåtande, information**
**Styrelsehandling nr 13**
Datum 2025-05-21
Ärendenummer BOS-2025-00190

Handläggare
Sara Fischer
Telefon: 031-731 50 10
E-post: sara.fischer@bostadsbolaget.se

# Årsrapport för dataskyddsarbetet 2024

## Informationsärende

## Styrelsen för Göteborgs stads bostadsaktiebolag

Informationen avseende årsrapport för dataskyddsarbetet 2024 antecknas.

## Sammanfattning

Årsrapporten för dataskyddsarbetet 2024 belyser flera viktiga aspekter av dataskyddsarbetet inom bolaget. Rapporten fokuserar på hur bolaget hanterar personuppgifter i enlighet med GDPR, de utmaningar som finns, samt de framsteg som gjorts under året. Årsrapporten innehåller också rekommendationer för framtida förbättringar och prioriteringar.

## Bedömning ur ekonomisk dimension

Ekonomiskt sett innebär ett starkt dataskyddsarbete att bolaget kan undvika kostsamma sanktioner och böter som kan uppstå vid bristande efterlevnad av GDPR. Genom att säkerställa att personuppgifter hanteras korrekt minskar risken för incidenter som kan leda till ekonomiska förluster och skada bolagets rykte.

## Bedömning ur ekologisk dimension

Även om dataskyddsarbete inte direkt påverkar den ekologiska dimensionen, kan digitalisering och effektiv hantering av data bidra till minskad pappersanvändning och därmed en mer hållbar verksamhet. Genom att implementera digitala lösningar som följer Dataskyddsförordningen kan bolaget minska sitt ekologiska fotavtryck genom att minska behovet av fysiska dokument och arkiv.

## Bedömning ur social dimension

Bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

## Samverkan

Ärendet har inte bedömts vara föremål för samverkan.

## Bilagor

1. Årsrapport för dataskyddsarbetet 2024

Dataskyddsenheten

Göteborgs Stad

# Årsrapport för dataskyddsarbetet 2024

## Göteborgs Stads Bostadsaktiebolag

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 fått kännedom om att det pågår en personalförändring avseende rollen som dataskyddskontakt inom bolaget. Dataskyddsombudet lyfte i samband med årsrapporten 2023 en risk med att dataskyddsarbetet inte bedrivs i samma utsträckning när den dåvarande dataskyddskontakten är frånvarande, vilket indikerar att dataskyddsarbetet till viss del är personberoende och därmed sårbart. Bolaget rekommenderas att säkerställa att den interna dataskyddsorganisationen ges rätt och tillräckliga resurser framåt samt att utveckla och stödja det arbete som bedrevs under den dåvarande dataskyddskontakten både nu och efter personalförändringen. Dataskyddsombudet ser också, utifrån verksamhets 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.

Under året har verksamheten gjort en leverantörsuppföljning där verksamheten uppger att en enkät har gått ut till bolagets största leverantörer med uppföljningsfrågor, vilket dataskyddsombudet ser som positivt. Dataskyddsombudet involverades initialt och lämnade råd och synpunkter på frågorna i enkäten. Dataskyddsombudet har dock inte tagit del av resultatet från uppföljning eller information om hur bolaget valt att följa upp eventuella brister hos leverantörerna och kan därmed inte uttala sig i denna del.

Inför årsrapporten uppger verksamheten även att en översyn och uppdatering av informationen på hemsidan har genomförts 2024. Vid en översiktlig genomgång av informationen bedömer dataskyddsombudet fortsatt att informationen behöver utvecklas ytterligare för att uppfylla kraven i art. 13 och 14 i GDPR. Eftersom bolaget har flera behandlingar som inte framgår av informationen på hemsidan ser dataskyddsombudet fortsatt att bolaget behöver göra en översyn av hur informationsplikten hanteras som helhet. En förutsättning för att bolaget ska kunna uppfylla kraven på information är också att behandlingsregistret är fullständigt samt att behandlingarna är väl definierade och avgränsade.

Under 2023 genomförde dataskyddsombudet en informationsinsats om informationsplikten och tillhandahöll såväl muntlig information som skriftligt underlag för stadens samtliga verksamheter. Bolaget uppmuntras att använda sig av underlaget som stöd i arbetet med informationsplikten.

Utöver ovan uppger verksamheten att en instruktion för kryptering av e-post och filer har uppdaterats och publicerats på intranätet. Dataskyddsombudet har inte involverats i arbetet, men ser att det är positivt att instruktioner för medarbetare tas fram.

# 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: Register över personuppgiftsbehandlingar

Verksamheten gavs följande rekommendationer:

- Komplettera behandlingsregistret med personuppgiftsbehandlingar som saknas och den information som krävs enligt artikel 30 i GDPR.

Kommentarer och rekommendationer:

I samband med uppföljningen uppger verksamheten att man både har sett över och uppdaterat behandlingsregistret under året. Dataskyddskontakten har även haft möten med medarbetare som ska sluta för att säkerställa att samtliga personuppgiftsbehandlingar som medarbetaren har arbetat med finns upptagna i behandlingsregistret. Verksamheten förklarar även att det finns en arbetsgång vid uppdatering av behandlingsregistret.

Under året har antalet behandlingar i behandlingsregistret ökat. Några personuppgiftsbehandlingar har försvunnit genom att bolaget exempelvis har kunnat slå ihop två behandlingar. Procentuellt upplever verksamheten att andelen behandlingar har ökat, men tycker det är svårt att uttala sig då det beror på hur behandlingar definieras.

Verksamheten uppger att bolaget kommer att byta systemstöd för behandlingsregistret framåt och att bolaget kommer göra ett omtag i och med övergången till det nya systemstödet.

Bolaget rekommenderas att se över hur behandlingarna i behandlingsregistret är definierade då det har betydelse för övriga delar av dataskyddsarbetet. Dataskyddsombudets anser inte att det inte är ändamålsenligt att behandlingar utgår från ett systemperspektiv. Vad gäller dokumenthanteringsplanen anser dataskyddsombudet att klassificeringsstrukturen och dokumenthanteringsplaner kan vara bra utgångspunkter i att ge vägledning för verksamheten när behandlingar ska identifieras. Samtidigt vill dataskyddsombudet vara tydlig med att dataskyddsombudet inte anser att en process i klassificeringsstrukturen kan översättas till en behandling rakt av. Vissa processer som framgår av klassificeringsstrukturen är inte personuppgiftsbehandlingar över huvud taget.

Eftersom behandlingsregistret är grundläggande i det övriga arbetet med dataskydd rekommenderas verksamheten, i likhet med flera andra verksamheter inom staden, att ta del av den stadengemensamma granskningsrapporten från dataskyddsombudets fördjupade kontroll och särskilt arbeta med sitt behandlingsregister utifrån rekommendationerna som framgår däri.

### Fokusområde 2: Konsekvensbedömning/samråd

Verksamheten gavs följande rekommendationer:

- Säkerställ att det finns en långsiktigt plan och prioritering för genomförandet av konsekvensbedömningar för behandlingar där en sådan krävs. Bolaget rekommenderas att framåt säkerställa att konsekvensbedömningar genomförs i praktiken.

Kommentarer och rekommendationer:

Enligt verksamheten finns utmaningar för bolaget att genomföra självständiga konsekvensbedömningar. Verksamheten uppger att de arbetar utifrån de förutsättningar som finns för att fullgöra bolagets skyldighet som personuppgiftsansvariga. Verksamheten upplever att de största utmaningarna handlar om att genomföra egna konsekvensbedömningar för stadengemensamma

system då bolaget saknar tillgång till all information från leverantören och där bolaget inte heller är med i dialogen med leverantören. Det är därför svårt att ställa krav på säkerhetsåtgärder eller ha full insyn i leverantörens upplägg av tjänster.

Enligt verksamheten finns en rutin för konsekvensbedömningar inom bolaget. Det finns även en plan att prioritera behandlingar som innefattar AI-teknik framåt och att tröskelanalyser ska genomföras för alla behandlingar som innefattar AI-teknik.

I arbetet med konsekvensbedömningar är det viktigt att medarbetare ges rätt och tillräckliga resurser för genomförandet. Dataskyddsombudet rekommenderar bolaget att se över prioriteringen av genomförandet av konsekvensbedömningar. Utifrån verksamhetens karaktär finns sannolikt befintliga personuppgiftsbehandlingar inom verksamhetens kärnverksamhet som bör prioriteras. Dataskyddsombudet rekommenderar att prioriteringen utgår från risker för registrerades fri- och rättigheter.

En förutsättning för att få en heltäckande överblick över vilka personuppgiftsbehandlingar som genomförs är att bolaget har ett komplett behandlingsregister med väl definierade och avgränsade behandlingar. Dataskyddsombudet rekommenderar därmed att bolaget i första hand fokuserar på behandlingsregistret, och i takt med att behandlingsregistret färdigställs, se över bolagets plan och prioritering för genomförandet av konsekvensbedömningar.

### Fokusområde 3: IT-system och digitala verktyg

Verksamheten gavs följande rekommendationer:

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

Kommentarer och rekommendationer:

Verksamheten uppger i samband med uppföljningen att verksamheten har arbetat med cookiehanteringen under året genom att uppdatera cookie-bannern.

Vid en översiktlig översyn av bolagets hemsida bedömer dataskyddsombudet att det finns ytterligare åtgärder som bör vidtas. Det handlar främst om samtyckesinhämtningen och informationen i samband med inhämtandet av samtycke.

Verksamheten rekommenderas att ta del av Post- och telestyrelsens (PTS) tillsynsbeslut avseende cookies från 2023. Bolaget kan även kontakta dataskyddsombudet för specifika råd och rekommendationer.

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

# 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: Dataskyddsorganisation

Säkerställa att den interna dataskyddsorganisationen inte ges mindre resurser än tidigare. Fortsätt att utveckla och stödja det arbete som bedrevs under den dåvarande dataskyddskontakten även nu och efter personalförändringen. Säkerställ att dataskyddsombudet involveras mer regelbundet i bolagets dataskyddsarbete.

- Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Ta del av den stadengemensamma granskningsrapporten från dataskyddsombudets fördjupade kontroll och arbeta med behandlingsregistret utifrån rekommendationerna som framgår av granskningsrapporten.

# 6 Bilagor

Bilaga 1: Kontrollplan för dataskyddsarbetet 2024–2025