Styrelsehandling 15
Älvstranden Utveckling AB
Diarienummer 0776/24
2025-02-07
Handläggare:
Ninni Tossavainen, Chef Verksamhetsstöd samt
Nina Maldevik Havner, dataskyddsombud
dataskyddsenheten på Intraservice

# Informationsärende – Årsrapport granskning av bolagets dataskyddsarbete

## Sammanfattning

Under 2024 har Stadens dataskyddsombud granskat hur Älvstranden Utveckling efterlever dataskyddsförordningen.

En del av denna granskning innebär att dataskyddsombudet har genomfört kontroller av dataskyddsarbetet inom den personuppgiftsansvariges organisation. Dessa kontroller specificeras genom en kontrollplan som innehåller tidplan och särskilda fokusområden för kontrollarbetet 2024.

Målsättningen är att detta ska bidra till att sätta fokus på verksamhetens dataskyddsarbete och därmed:

1. Säkerställa ett kontinuerligt dataskyddsarbete som skapar förutsättningar för efterlevnad av förordningen.
2. Maximera ett riskbaserat arbetssätt och därigenom minimera risken för lagbrott.
3. Göra dataskyddsarbetet till en integrerad del i verksamhetens informationssäkerhetsarbete.

Nina Maldevik Havner, representant för Dataskyddsombudet Intraservice, informerar om vad hon sett i granskningen av bolagets dataskyddsarbete på sammanträdet.

## Bedömning av ärendets principiella beskaffenhet

Bolaget bedömer att ärendet inte är av principiell beskaffenhet.

## Bilagor

Bilaga 1. Årsrapport granskning av Älvstranden Utvecklings dataskyddsarbete 2024.

Göteborgs Stad

# Årsrapport för dataskyddsarbetet 2024

## Älvstranden Utveckling 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 förvaltningsnivå2, 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 personuppgiftsincidenter, uppdatering av bolagets information och andra dataskyddsfrågor hänförliga till granskning.

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.

## 3.2 Särskilda iakttagelser

### 3.2.1 En sårbar dataskyddsorganisation

Bolaget uppger att en pågående intern omorganisation är så gott som klar och att en av två bolagets dataskyddskontakter kommer att sluta sin anställning.

Även inom verksamheter med låga risker, generellt utifrån storlek och kärnområden, krävs kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

Bolaget påvisar en sårbarhet när hanteringen centreras kring en person. Förtydligande ansvar, rutiner och processer som flera anställda är tränade i kan till viss del förhindra dessa risker.

Dataskyddsombudet rekommenderar därför att bolaget ser över resurstillsättningen och säkerställer ett systematiskt dataskyddsarbete där dataskyddsombudet involveras i alla frågor rörande dataskydd.

# 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:

Verksamheten rekommenderas uppdatera registret med samtliga behandlingar samt säkerställa arbetssätt för uppdatering vid tillkomsten av nya eller förändrade behandlingar.

Kommentarer och rekommendationer:

Av uppföljningen framgår att bolaget har arbetat med behandlingsregistret under året vilket är positivt även om dataskyddsombudet inte har tagit del av bolagets behandlingsregister. Bolaget uppger i sin kompletterande kommentar att ny dataskyddskontakt inte är utsedd dock att avdelningschefen för HR Compliance kommer att vara t. f. dataskyddskontakt enligt bolagets ordning. Vidare uppges att en ny documentcontroller kommer att anställas under 2025 dock oklart om dataskyddsfrågorna ska ligga där. Eftersom arbetet med processer och ägandeskap pågår kommer behandlingsregistret att uppdateras först därefter.

Dataskyddsombudet anser att uppföljningen visar att bolaget behöver arbeta mera skyndsamt och involvera fler medarbetare kring pågående uppdatering.

Dataskyddsombudet rekommenderar att bolaget tar del av den generella granskningsrapporten från dataskyddsombudets fördjupade kontroll och beaktar rekommendationerna som framgår däri vid arbete med sitt behandlingsregister.

### Fokusområde 2: Konsekvensbedömning/samråd

Verksamheten gavs följande rekommendationer:

Verksamheten rekommenderas ta fram arbetssätt och ett helhetsgrepp för att identifiera riskfyllda behandlingar som inbegriper genomförande, dokumentation och uppföljning liksom dataskyddsombudets uttalande.

Kommentarer och rekommendationer:

Av uppföljningen framgår att bolaget har missuppfattat vad som gäller och när en konsekvensbedömning behövs liksom praktisk arbetsgång. Bolaget uppger att ett omtag är på gång och att bolaget kommer att involvera och inhämta dataskyddsombudets skriftliga synpunkter framgent när väl bolagets nya dataskyddsorganisation är klar.

Uppföljningen visar att dataskyddsombudets rekommendation kvarstår och kommer att följas upp under 2025.

### Fokusområde 3: IT-projekt och upphandling

Verksamheten gavs följande rekommendation:

Verksamheten rekommenderas ta fram rutiner för att via kravställning säkerställa skyddet av personuppgifter och säkerställa följsamhet mot GDPR vad gäller inbyggt dataskydd och dataskydd som standard samt att involvera dataskyddsombudet från uppstart.

Kommentarer och rekommendationer:

Bolaget uppger att kontakt har etablerats med INK för att få med nödvändiga krav och formuleringar vid framtida upphandlingar som en av åtgärderna för att säkerställa inbyggt dataskydd och dataskydd som standard och att man kommer att jobba vidare i enlighet med årsrapportens rekommendationer.

Dataskyddsombudet har inte involverats i någon upphandling under det gångna året och utgår från att rekommendationen är omhändertagen utifrån uppföljningen och att bolaget kontaktar dataskyddsombudet om och när en upphandling blir aktuell.

# 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 1: Dataskyddsorganisation

Ser över resurstillsättningen och säkerställa ett systematiskt dataskyddsarbete där dataskyddsombudet involveras i alla frågor rörande dataskydd.

- Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Uppdatera registret med samtliga behandlingar samt säkerställa arbetssätt för uppdatering vid tillkomsten av nya eller förändrade behandlingar. Vidare ta del av den generella granskningsrapporten från dataskyddsombudets fördjupade kontroll och beakta rekommendationerna som framgår däri vid arbete med behandlingsregistret.

- Kontrollpunkt 9: Konsekvensbedömningar/samråd

Ta fram arbetssätt och ett helhetsgrepp för att identifiera riskfyllda behandlingar som inbegriper genomförande, dokumentation och uppföljning liksom dataskyddsombudets uttalande.

# 6 Bilagor

Bilaga 1: Kontrollplan för dataskyddsarbetet 2024–2025