Tjänsteutlåtande, information
Styrelsehandling nr 18
Utfärdat 2025-04-01
Diarienummer: 2025 - 00047

Handläggare
Linda Björk
Telefon:031-773 75 56
E-post: linda.bjork@framtiden.se

.

Årsrapport för dataskyddsarbetet 2024

Informationsärende

Styrelsen Förvaltnings AB Framtiden

Årsrapport för dataskyddsarbetet 2024 antecknas.

Ärendet

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras i artikel 39 i GDPR. I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud för förvaltningar och bolag

Dataskyddsombudet ska ge råd, rekommendationer och informera om frågor som rör behandlingar av personuppgifter. Dataskyddsombudet har även i uppdrag att oberoende granska verksamheternas arbete med dataskyddsfrågor för att säkerställa att dataskyddslagstiftningen efterlevs.

Dataskyddsombudet lämnar årligen en rapport om verksamhetens dataskyddsarbete till varje nämnd och bolag i Göteborgs Stad. I rapporten redogör dataskyddsombudet för de iakttagelser som gjorts och det kontrollarbete som genomförts.

Dataskyddsenheten rekommenderar bolaget att under 2025 prioritera följande delar av dataskyddsarbetet:

- Se över hur dataskyddsombudet kan involveras mer aktivt i dataskyddsarbetet inom koncernen.
- Ta del av den stadengemensamma granskningsrapporten från dataskyddsombudets fördjupade kontroll och arbeta med behandlingsregistret utifrån

Framtiden delar inte dataskyddsombudets bild av att ansvarsfördelningen mellan koncernens bolag är otydlig utifrån ett dataskyddsperspektiv. Ansvaret för dataskyddsfrågorna ligger hos respektive dotterbolag och med anledning av föreliggande rapport har koncernledningen informerats om ansvaret.

Framtiden har med utgångspunkt i rekommendationerna och de åtgärder som vidtagits under 2024 tagit fram en åtgärdsplan för 2025 som redovisas till styrelsen i ett separat ärende på föreliggande sammanträde.

Bedömning ur ekonomisk, ekologisk och social dimension

Ärendet är av administrativ karaktär och bolaget har därför inte funnit några särskilda aspekter på frågan utifrån dessa dimensioner.

Samverkan

Ärendet har inte varit föremål för samverkan.

Bilaga

Årsrapport för dataskyddsarbetet 2024

Göteborgs Stad

Styrelsehandling nr 18
Bilaga 1
2025-04-01

Årsrapport för dataskyddsarbetet 2024

Förvaltnings AB Framtiden

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

Under året har kontakten mellan dataskyddsombudet och bolaget främst utgjorts av deltagande vid Framtidenskoncernens gruppmöten inom dataskydd, där representanter för de olika bolagen deltar. Utöver det har dataskyddsombudet även haft en dialog med verksamheten i arbetet med bolagskonsolideringen. Därtill har dataskyddsombudet och bolaget initierat ett inledande informationsutbyte kring koncernstrukturen och rådsstrukturen inom bolaget samt dataskyddsombudets roll. Dataskyddsombudets förhoppning är att dialogerna kan fortsätta att utvecklas under 2025 då arbetet som genomförs inom koncernens råd och frågor som diskuteras kopplat till dataskydd sannolikt har betydelse för det löpande arbetet, både för koncernen som helhet, och för enskilda dotterbolags fortsatta arbete i specifika frågor.

Även om dataskyddsombudet inte har kontrollerat bolagets dataskyddsorganisation särskilt, så var dataskyddsombudet uppfattning i samband med årsrapporten 2023 att bolagets dataskyddsorganisation är väl organiserad och att det fanns förutsättningar för att kunna bedriva ett systematiskt dataskyddsarbete. Då det pågår en personalförändring som har betydelse för dataskyddsorganisationen är det av särskild vikt att bolaget framåt arbetar för att bibehålla de organisatoriska förutsättningar som dataskyddsombudet har uppfattat finns.

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: Dataskyddsorganisation

Verksamheten gavs följande rekommendationer:

- Se över hur dataskyddsombudet kan involveras mer aktivt i dataskyddsarbetet inom koncernen, inklusive i det arbete som bedrivs inom ramen för ”Säkerhetsrådet”, med syftet att säkerställa att bolagen inom koncernen ges förutsättningar för att uppfylla kraven enligt artikel 38 i GDPR.

Kommentarer och rekommendationer:

Som framgår under avsnitt 3.1 har dataskyddsombudet och bolaget initierat ett inledande informationsutbyte kring koncernstrukturen och rådsstrukturen samt dataskyddsombudets roll där det har varit ett första möte under hösten.

I samband med uppföljningen uppger verksamheten att alla bolag inom koncernen har ett långtgående självbestämmande. I vissa frågor kan koncernledningen (koncernledningsgruppen med alla bolagens VD:ar) ta beslut. Det förekommer dock missuppfattningar bland vissa av bolagens handläggare att moderbolaget har tagit vissa beslut, trots att så inte är fallet. Även dataskyddsombudet har fått indikationer på att dotterbolagen i vissa fall hänvisar till moderbolaget. Om det råder oklarheter, anser dataskyddsombudet att det är av vikt att oklarheterna reds ut inom koncernen eftersom hur och av vem/vilka besluts tas eller hur styrning sker har betydelse vid bedömningen av ansvarsfördelningen ur ett dataskyddsperspektiv mellan bolagen.

Mot bakgrund av att det endast har varit en inledande och övergripande dialog kommer rekommendationen om att se över hur dataskyddsombudet kan involveras mer aktivt i dataskyddsarbetet inom koncernen att kvarstå. Dataskyddsombudet ser dock att det är mycket positivt att ett inledande informationsutbyte har inletts och bedömer att det framåt behöver utvecklas. Rekommendationen tillställs bolaget, då det främst är moderbolaget som främst leder/är sammankallande för koncernens råd.

Fokusområde 2: Register över personuppgiftsbehandlingar

Verksamheten gavs följande rekommendationer:

- Gör en översyn av befintligt register. Gå igenom hur de dokumenterade behandlingarna är definierade och kontrollera för respektive behandling att informationen uppfyller kraven enligt artikel 30 i GDPR.

Kommentarer och rekommendationer:

Under våren lyfte bolaget ut behandlingsregistret från Draftit till en tillfällig excel-fil i väntan på ett nytt stadengemensamt systemstöd. Under uppföljningen framkom att det har varit planerat att göra en riktad insats kring behandlingsregistret på koncernnivå med start under oktober 2024. Tidigare har bolaget fått till sig att det nya systemstödet skulle kunna användas redan från hösten 2024 i form av en särskild testfas, men koncernen har nyligen fått besked om att så inte kommer att kunna ske.

Bolaget vill få in en helt ny struktur på behandlingsregistret där de önskar finnas en tydlig koppling mellan behandlingar, informationssäkerhet och dokumenthantering samt en sammanhållen dokumentation i ett vidare informationssäkerhetsperspektiv.

Arbetet med behandlingsregistret har dock fått pausats i väntan på det nya systemstödet. När koncernens bolag har fått information om vilken dataarkitektur som ska bli gällande kan importdata förberedas innan systemet är i drift.

Verksamheten har därför valt att inte göra några större förändringar i sitt behandlingsregister förrän de vet vilken indata eller vilken data som kan importeras till det nya systemstödet. Detta är för att inte riskera att behöva göra resurskrävande ändringar igen vid ett senare tillfälle.

Även om dataskyddsombudet har förståelse för att bolaget inväntar ett nytt systemstöd finns det viss information som behöver finnas i behandlingsregistret för att kraven i art. 30 i GDPR ska anses vara uppfyllda. Oavsett om behandlingsregistret finns i en excel-fil eller ett systemstöd behöver informationen hållas uppdaterad. Utifrån dataskyddsombudets fördjupade kontroll har en stadengemensamma granskningsrapport sammanställts. I likhet med andra verksamheter i staden, rekommenderas bolaget att ta del av den stadengemensamma granskningsrapporten och arbeta med sitt behandlingsregistret utifrån rekommendationerna som framgår av granskningsrapporten.

Fokusområde 3: Informationsplikt

Verksamheten gavs följande rekommendationer:

- Se över samtliga delar i den information som lämnas till de registrerade och de arbetssätt som tillämpas för att säkerställa att informationsplikten gentemot de registrerade uppfylls. I arbetet behöver de rekommendationer som tidigare lämnats kopplat till den specifika informationen i integritetspolicyn omhändertas.

Kommentarer och rekommendationer:

Enligt uppgifter från bolaget är planen att se över informationsplikten när behandlingsregistret har setts över.

Vad gäller informationsplikten har verksamheten idéer på att försöka få till någon form av export från behandlingsregistret. Långsiktigt är att det ska vara möjligt att koppla samman informationen i behandlingsregistret och den information som behöver lämnas enligt informationsplikten. För varje enskild behandling ska den specifika informationen som finns i behandlingsregistret också kunna användas i integritetsinformationen.

Utöver det nämnda har inget mer arbete gjorts kring informationsplikten i väntan på det nya systemstödet för behandlingsregistret. Det finns dock en skriftlig plan för arbetet med informationsplikten framåt.

Då dataskyddsombudet delar bolagets bedömning av att behandlingsregistret är en förutsättning för ett effektivt arbete med informationsplikten rekommenderas bolaget att först och främst särskilt arbeta med behandlingsregistret under 2025. I takt med att behandlingsregistret färdigställs, rekommenderas bolaget att uppdatera sin information. Utifrån vad som framkommer på uppföljningen kvarstår dock dataskyddsombudets rekommendationer från årsrapporten 2023.

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): Integritetspolicy

Verksamheten gavs följande rekommendationer:

- Komplettera med information om att den registrerade kan få ta del av mer information om intresseavvägningsbedömningen i den externa integritetspolicyn för de behandlingar som baseras på berättigat intresse/intresseavvägning enligt art. 6.1 f GDPR.
- Förtydliga rättslig grund för behandlingarna i den information som lämnas till anställda.
- Tydliggör lagringstid för respektive behandling i såväl den externa integritetspolicyn som i informationen till anställda.
- Säkerställ att samtliga behandlingar, där personuppgifterna inte samlas in direkt från den registrerade, kompletteras med information om kategorier av personuppgifter och var personuppgifterna kommer ifrån.
- Förtydliga vad som gäller avseende de registrerades rättigheter och specificera för respektive behandling, primärt i den externa integritetspolicyn. Förtydliga också kring rätten att invända mot en behandling i tillämpliga fall.
- Förtydliga informationen om tredjelandsöverföring i den externa integritetspolicyn och se till att informationen finns även i den information som lämnas till anställda.
- Säkerställ att den externa integritetspolicyn är heltäckande och innehåller alla behandlingar eller säkerställ att information lämnas till de registrerade på annat vis.
- Säkerställ att den externa integritetspolicyn och informationen har ett tydligt språk och inte innehåller bestämningsord såsom ”kan” och liknande.

Kommentarer och rekommendationer:

Som framgår under fokusområde 3 avvaktar bolaget att arbeta med informationsplikten i väntan på det nya systemstödet för behandlingsregistret. Enligt verksamheten finns dock en skriftlig plan framåt för arbetet. Rekommendationer som gavs i samband med den fördjupade kontrollen kommer därför att kvarstå och uppföljning kommer att ske i igen 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: Dataskyddsorganisation

Se över hur dataskyddsombudet kan involveras mer aktivt i dataskyddsarbetet inom koncernen.

- 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

Göteborgs Stad

Kontrollplan för dataskyddsarbetet 2025–2026

Förvaltningar och bolag i Göteborgs Stad

2025-02-26

Innehåll

1 Bakgrund

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. Att förvaltningar och bolag hanterar personuppgifter i enlighet med gällande lag bör vara en självklarhet i syfte att visa omsorg om det förtroende som givits den som har att hantera personuppgifter.

Det är varje nämnd och bolaget 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. Dataskyddsombudet har särskild sakkunskap i dataskyddslagstiftning och arbetar bland annat för att hålla nämnden/bolaget informerade om hur verksamheten lever upp till dataskyddslagstiftningen. Vad som är dataskydds-ombudets uppgifter framgår direkt av GDPR. En av dessa uppgifter är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. När dataskyddsombudet kontrollerar efterlevnaden av dataskyddslagstiftningen sker det bland annat genom att samla in information om hur personuppgifter behandlas inom en verksamhet och genom att kontrollera hur bestämmelser och interna styrdokument som styr dataskyddsarbetet efterlevs.

1.1 Ändrad utformning av den övergripande kontrollen 2025

Med anledning av den omorganisation som genomfördes hösten 2024, där tre tjänster flyttades från dataskyddsenheten till stadsledningskontorets dataskyddsfunktion, har dataskyddssenheten behövt arbeta om strukturen för kontrollarbetet. Under 2024 visades det genom ett ändrat upplägg för den fördjupade kontrollen, och under 2025 kommer det visas genom ändringar i utformningen av den övergripande kontrollen.

Den övergripande kontrollen kommer fortfarande att genomföras inom alla verksamheter under hösten 2025, men dess utformning och omfattning kommer att skilja sig från tidigare år. Ändringarna syftar till att öka kvaliteten i kontrollen och möjliggöra för mer systematisk uppföljning av verksamheternas dataskyddsarbete.

Dataskyddsenheten kommer innan kontrollen genomförs att skicka ut information om ändringarna till verksamheterna.

2 Kontrollarbetet 2025–2026

Den övergripande och viktigaste uppgiften för dataskyddsombudet är att övervaka att organisationen följer dataskyddsförordningen. I Göteborgs Stad innebär detta bland annat att dataskyddsombudet genomför kontroller av dataskyddsarbetet inom förvaltningar och bolag. För dataskyddsombudet är kontrollarbetet ett sätt att få en bild av vilka risker och/eller brister som eventuellt föreligger inom en verksamhet. Genom kontroller kan dataskyddsombudet kartlägga verksamhetens dataskyddsarbete, och denna kartläggning kan sedan användas som ett stöd av verksamheten i dess fortsatta arbete med dataskydd. Dessa kontroller specificeras genom denna kontrollplan, som syftar till att informera personuppgiftsansvariga om upplägg och tidplan för kontrollarbetet åren 2025 och 2026. Dataskyddsombudets kontrollarbete löper över tvåårsperioder. En ny kontrollplan skickas ut årligen, vilken omfattar både innevarande och nästkommande kalenderår.

Syftet med att arbeta utefter en på förhand fastställd kontrollplan är att det ska bidra till att sätta fokus på verksamhetens dataskyddsarbete och därmed:

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

2.1 Kontrollarbetets delar

Kontrollarbetet består av tre delar som tillsammans syftar till att ge, såväl dataskyddsombud som personuppgiftsansvariga, en överblick över verksamhetens dataskyddsarbete och dess följsamhet gentemot GDPR.

2.1.1 Övergripande kontroll

Den övergripande kontrollen utgår från principerna om inbyggt dataskydd och dataskydd som standard (enligt artikel 25 i GDPR). Verksamhetens följsamhet mot förordningen beror till stor del på hur väl dessa principer har integrerats i ordinarie arbetsprocesser. Med principerna som utgångspunkt har tolv kontrollpunkter identifierats. Dessa är av både teknisk och organisatorisk karaktär och är gemensamma för alla verksamheter inom Göteborgs Stad.

Den övergripande kontrollen genomförs genom en enkät inom vilken verksamhetens dataskyddsarbete kartläggs. Resultaten från enkäten är tänkt att ge en generell ögonblicksbild för respektive kontrollpunkt och kan därför, förutsatt att enkäten är korrekt ifylld, användas som vägledning för verksamheten i sitt dataskyddsarbete. Syftet är att få till ett långsiktigt och systematiskt arbetssätt, samt åskådliggöra de förändringar som vidtas över tid.

För beskrivning av de olika kontrollpunkterna, se bilaga 1.

2.1.2 Fördjupad kontroll

I utformningen av den fördjupade kontrollen utgår dataskyddsombudet från de risker som identifierats, både inom enskilda verksamheter och på en övergripande nivå. Hänsyn tas även till vad som bedöms kunna få störst effekt för flest verksamheter inom Staden. Från och med 2024 är den fördjupade kontrollen utformad som en stickprovskontroll vilket innebär att inte alla verksamheter kontrolleras. I stället genomförs kontrollen inom ett antal förvaltningar och bolag som dataskyddsombudet anser utgör ett representativt urval för stadens verksamheter.

Resultaten från kontrollen redovisas dels på verksamhetsnivå genom en rapport till respektive deltagande verksamhet, dels på övergripande nivå genom en staden gemensam rapport. Den staden gemensamma rapporten är tänkt att kunna användas av flera verksamheter och genom denna kan även de verksamheter som ej varit med i kontrollen dra nytta av resultaten.

2.1.3 Uppföljning

Uppföljning av de rekommendationer som tidigare lämnats till verksamheten i samband med årsrapportering eller fördjupade kontroller genomförs årligen. Resultatet redovisas till styrelse eller nämnd i verksamhetens årsrapport.

2.2 Tidplan för kontrollarbetet 2025–2026

I tabellerna nedan anges huvuddragen i kontrollarbetet för åren 2025–2026 för stadens förvaltningar och bolag.

2025	Aktivitet
Februari	Kontrollplan för 2025–2026 lämnas till nämnder och styrelser.
September	Övergripande kontroll genomförs.
November – december	Genomgång av innehåll i årsrapport med respektive verksamhet.
December	Dataskyddsombudets årsrapport översänds till nämnd eller styrelse.

2026	Aktivitet
Februari	Kontrollplan för 2026–2027 lämnas till nämnder och styrelser.
April – Oktober	Fördjupad kontroll genomförs.
November – december	Genomgång av innehåll i årsrapport med respektive verksamhet.
December	Dataskyddsombudets årsrapport översänds till nämnd eller styrelse.

3 Rapportering

3.1 Årsrapport

Det är nämnd respektive bolag som har det yttersta ansvaret för att verksamheten följer dataskyddslagstiftningen och dataskyddsombudet ska enligt lag rapportera om detta till högsta förvaltningsnivå. Därför sammanställer dataskyddsombudet årligen en rapport om verksamhetens dataskyddsarbete. I rapporten redogörs för eventuella risker och brister som dataskyddsombudet har identifierat. I rapporten redogörs också för de råd och rekommendationer som dataskyddsombudet har lämnat. För att möjliggöra en direkt kommunikation mellan dataskyddsombud och högsta ansvarsnivå inom verksamheten ska årsrapporten tillhandahållas nämnd respektive bolagsstyrelse.

3.2 Särskilt yttrande

Dataskyddsombudet kan i vissa situationer komma att rikta ett särskilt yttrande till högsta ansvarsnivå. En sådan situation kan vara om dataskyddsombudet har identifierat höga risker för de registrerade som kräver omgående åtgärder från ansvarig nämnd/bolag. Det kan också vara om dataskyddsombudet uppmärksammar att det inom verksamheten fattats beslut som är oförenliga med dataskyddslagstiftningen och dataskyddsombudets råd.

Kontakt

Frågor avseende kontrollplanen hänvisas till dataskyddsenhetens funktionsbrevlåda; dso@intraservice.goteborg.se.

Bilaga 1 - Beskrivning av fasta kontrollpunkter

Kontrollpunkt 1: Dataskyddsorganisation

Kontrollpunkten avser verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete och omfattar bland annat verksamhetens dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt tillhandahållna resurser för arbetet.

Kontrollpunkt 2: Personuppgiftsincidenter

Kontrollpunkten avser verksamhetens förutsättningar för att identifiera och hantera personuppgiftincidenter. För att uppfylla ansvarsskyldigheten bör verksamhetens rutin för hanteringen vara dokumenterad. I de fall verksamheten är både personuppgiftsansvarig och personuppgiftsbiträde bör rutinen omfatta båda scenarier. I kontrollpunkten ingår även översyn av verksamhetens rutin för att bedöma incidenter, hantering av eventuell anmälan till tillsynsmyndigheten, samt hur rutinerna tillgängliggörs och kommuniceras inom verksamheten. Även efterlevnad av verksamhetens dokumentationsskyldighet, att alla inträffade personuppgiftsincidenter registreras, innefattas.

Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Kontrollpunkten avser verksamhetens dokumentation av biträdesavtal och andra överenskommelser gällande dataskydd och förutsätter att verksamheten har identifierat samt registrerat personuppgiftsbiträden i personuppgiftsregistret. Även verksamhetens rutiner för uppdatering och uppföljning av tecknade biträdesavtal innefattas.

Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även verksamhetens arbete med, och rutin för, att säkerställa ett uppdaterat och heltäckande register innefattas.

Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Kontrollpunkten avser verksamhetens övergripande styrning för att arbeta med dataskydd. Tydlig styrning sätter ramarna för arbetet med dataskydd och främjar ett riskbaserat arbetssätt. Kontrollpunkten innefattar även verksamhetens arbete för att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet, samt hur verksamheten arbetar med egna interna kontroller för att säkerställa att dataskyddslagstiftningen efterlevs.

Kontrollpunkt 6: Utbildning

Kontrollpunkten avser verksamhetens arbete med att utbilda och upprätthålla kunskapsnivån i dataskyddsfrågor hos anställda.

Kontrollpunkt 7: Informationsplikt

Kontrollpunkten avser hur väl verksamheten uppfyller principen om öppenhet och kravet på att lämna information till de registrerade om hur deras person-uppgifter behandlas. Punkten omfattar även hur verksamheten säkerställer att informationen är uppdaterad.

Kontrollpunkt 8: E-post och dokumenthantering

Kontrollpunkten avser verksamhetens rutiner för e-post och dokumenthantering. I detta är en aktuell och fastställd dokumenthanteringsplan med gallringsbeslut en förutsättning för att verksamheten ska kunna säkra följsamhet gentemot dataskyddslagstiftningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Kontrollpunkt 9: Konsekvensbedömning/samråd

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras samt genomföra denna. Även verksamhetens rutiner för arbetet med konsekvensbedömningar samt hur dataskyddsombudet involveras i arbetet ingår. Därtill tillkommer verksamhetens rutin för att hantera de risker som identifieras i konsekvensbedömningen, samt hur genomförda konsekvensbedömningar följs upp och hålls aktuella.

Kontrollpunkt 10: IT-projekt och upphandling

Kontrollpunkten avser verksamhetens organisation och rutiner för hantering av dataskyddsfrågor inom IT-projekt och upphandling. I detta ingår till exempel hur verksamheten integrerar dataskyddsfrågor i arbetet med upphandling av nya, samt utvecklingen av, befintliga system och tjänster.

Kontrollpunkt 11: IT-system och digitala verktyg

Kontrollpunkten avser verksamhetens rutiner för att säkerställa att verksamhetens personuppgiftshantering inom ramen för IT-system och digitala verktyg är förenlig med dataskyddslagstiftningen. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår även.

Kontrollpunkt 12: Hantering av registrerades rättigheter

Kontrollpunkten avser verksamhetens förutsättningar för att hantera de registrerades rättigheter. En förutsättning för att verksamheten ska kunna hantera de registrerades rättigheter är att man har en process och rutiner för arbetet, så att den registrerades personuppgifter enkelt kan lokaliseras vid efterfrågan. Även verksamhetens rutin för att hantera ett tillbakadragande av samtycke ingår i kontrollpunkten.