Göteborgs Stad

Årsrapport för dataskyddsarbetet 2025

Göteborgs spårvägar AB

2025-12-18

Innehåll

1 Inledning

Dataskyddsförordningen (GDPR) tillkom för att särskilt skydda människors rätt till integritet, samt var och ens rätt till insyn i 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. Dataskyddsreglerna styr hur personuppgifter får samlas in, användas och hanteras för att säkerställa att uppgifterna används korrekt och rättvist. Lagstiftningen finns till för att skydda individen från skada och sätter ramarna för hur personuppgifter får behandlas i en alltmer digital värld.

1.1 Göteborgs Stads dataskyddsombud

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 oberoende övervaka och granska att stadens förvaltningar och bolag följer dataskyddslagstiftningen. Dataskyddsombudet har också till uppgift att ge råd och stöd till förvaltningar och bolag i dataskyddsfrågor.

Det är varje nämnd och bolag som är ytterst ansvarig för att dess verksamhet följer dataskyddslagstiftningen. Utifrån detta, och då dataskyddsombudet enligt lag ska rapportera om arbetet till högsta förvaltningsnivå, 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 och årets kontrollarbete, samt för resultatet av den uppföljning som genomförts av hur verksamheten hanterat och arbetat med de rekommendationer som lämnats tidigare. Årsrapporten är avsedd att kunna användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd.

1.2 Ändringar i kontrollarbetet 2025

I kontrollplanen för 2025–2026 aviserades att utformningen av den övergripande kontrollen skulle revideras under 2025. Revideringen innebär att kontrollpunkterna är tio i stället för tolv, samt att antalet frågor att besvara för varje kontrollpunkt är färre.[2] Kontrollpunkterna utgår även fortsättningsvis ifrån principerna i GDPR.

Syftet med ändringarna är att skapa bättre förutsättningar för dataskyddsenhetens uppföljningsarbete och rapportering till nämnder/styrelser, samt att förtydliga och förenkla verksamheternas arbete med kontrollen. Genom tydligare kontrollpunkter och enkätfrågor är dataskyddsenhetens förhoppning att resultatet av kontrollen ska kunna utgöra ett bättre stöd för verksamheterna i deras eget dataskyddsarbete.

[1] Artikel 39 i GDPR.
[2] Se bilaga 1 för information om reviderade kontrollpunkter.

2 Stadenövergripande iakttagelser 2025

2.1 Arbete med digitalisering och AI kräver dataskyddsresurser

Dataskyddsenheten har under året fortsatt kunnat konstatera att många verksamheter inte avsätter de resurser som krävs utifrån dataskydd i projekt som rör digitalisering och AI. Detta medför att dataskyddsperspektivet kommer in alldeles för sent vid införandet av nya tekniska lösningar. Då många initiativ inom digitalisering och AI drivs i projektform finns ofta en utarbetad tidsplan som verksamheterna förhåller sig till. Om verksamheten inte har med dataskyddsperspektivet från start i dessa projekt, innebär det även att dataskyddsenheten involveras i ett skede där det ofta redan är bestämt hur en personuppgiftsbehandling ska genomföras. Om dataskyddsenheten då har synpunkter på personuppgiftsbehandlingen, innebär det att verksamheten inte har möjlighet utifrån sin tidsplan att omhänderta dessa synpunkter. Eftersom dataskyddsenheten inte utgår från verksamhetens tidsplan, utan fokuserar på att säkerställa att dataskyddsperspektivet omhändertas, blir följden av detta många gånger irritation och att dataskydd ses som ett hinder för verksamhetsutveckling. Utifrån dataskyddsenhetens perspektiv är det dock inte dataskyddslagstiftningen som är problemet, utan problemet ligger i stället i att verksamheterna inte har tillräckliga resurser eller kunskap nog för att omhänderta dataskyddsperspektivet inom ramen för sitt digitaliseringsarbete.

Dataskyddsenheten vill i sammanhanget påminna stadens verksamheter att det är den personuppgiftsansvariges skyldighet att involvera dataskyddsombudet i god tid i frågor som rör skyddet av personuppgifter.[3] Detta innebär att det är viktigt att stadens verksamheter tar ansvar för att på ett korrekt sätt och i god tid involvera dataskyddsombudet i alla frågor som rör skyddet av personuppgifter. Om dataskyddsperspektivet fortsätter förbises i digitaliseringsarbetet, kommer det på sikt att ge upphov till uppenbara risker för de registrerades fri- och rättigheter.

2.2 Årets incidenter visar på betydelsen av grundläggande dataskyddsarbete

Under året har det inträffat flera större personuppgiftsincidenter inom verksamheter i Göteborgs Stad. En del incidenter har omfattat större delen av Stadens verksamheter, medan andra varit verksamhetsspecifika. Oavsett omfattning har alla incidenter tydligt visat på hur viktigt det är att verksamheten har koll på sina personuppgiftsbehandlingar. Här har dataskyddsenheten under året tyvärr kunnat

[3] Detta ansvar framgår av artikel 38.1 i GDPR.

konstatera att det finns stora brister inom många av stadens förvaltningar och bolag.

En grundläggande förutsättning för att en verksamhet ska kunna hantera en personuppgiftsincident är att verksamheten har koll på vilken eller vilka personuppgiftsbehandlingar incidenten gäller, samt hur ansvarsfördelningen för behandlingen ser ut. Detta är nödvändigt för att verksamheten ska kunna veta vilka registrerade samt vilka personuppgifter som incidenten omfattar, och utifrån det kunna genomföra en riskbedömning som i sig styr hur incidenten ska hanteras. En felaktig riskbedömning skulle kunna resultera i en bristande incidenthantering och medföra ytterligare risker för de registrerade.

En följd av de inträffade personuppgiftsincidenterna, och den uppmärksamhet som dessa har fått, är att antalet registrerade som vill utöva sina rättigheter och begär registerutdrag eller att deras uppgifter raderas har ökat. Även i verksamheters hantering av dessa har dataskyddsenheten kunnat konstatera brister kopplat till att det inom vissa verksamheter saknas kunskap om vilka personuppgiftsbehandlingar som utförs eller att verksamheter saknar möjligheter att tekniskt söka fram de personuppgifter som finns. Särskilt tydligt har detta visats efter incidenten hos stadens leverantör Miljödata, som utöver detta även aktualiserade frågor om interna biträdesrelationer och enskilda verksamheters möjligheter för att bestämma över hanteringen av sin information. Dataskyddsenheten kan konstatera att flera av de identifierade bristerna som aktualiserats i ljuset av dessa incidenter har påpekats av dataskyddsenheten tidigare. Dataskyddsenheten hoppas att årets inträffade incidenter blir en väckarklocka för förvaltningar och bolag i Göteborgs Stad, och att verksamheterna framåt prioriterar arbetet med grundläggande delar, som behandlingsregister och information till registrerade, i deras interna dataskyddsarbete.

I skrivande stund har Integritetsskyddsmyndigheten (IMY) inlett en tillsyn av Göteborgs Stad med anledning av incidenten hos Miljödata. Dataskyddsombudet förutsätter att Stadens verksamheter följer ärendet och framåt vidtar eventuella åtgärder utifrån resultatet av tillsynen.

3 Verksamhetsspecifika iakttagelser 2025

3.1 Verksamhetens dataskyddsarbete

Under de senaste åren har Göteborgs Spårvägars (GS) dataskyddsarbete tagit stora kliv framåt. Verksamheten har haft stöd av en konsult inom området som bidragit med mycket värdefull kunskap. I 2024 års årsrapport konstaterade dataskyddsombudet att bolagets stora utmaning var att säkerställa att den höjda nivån på dataskyddsarbetet kunde bibehållas även efter att den konsult man haft inne avslutat sitt uppdrag. Det framgår också av bolagets svar på dataskyddsombudets kontrollfrågor att dataskyddsarbetet delvis varit personberoende, och att det systematiska arbetet haft svårt att få genomslag i organisationen. Dataskyddsombudet lyfte också att den interna dataskyddsorganisationen behövde tillföras kompetens, och det systematiska dataskyddsarbetet behöver integreras i verksamheten. Ett viktigt steg i detta är att fastställa formerna för hur organisationen ska arbeta med dataskydd i form av dokumenterade arbetssätt och rutiner som förankras hos högsta ledningen.

Under stora delar av året har verksamheten saknat dedikerad resurs för dataskyddsarbetet, efter att den konsult som GS haft inne gått vidare till andra uppdrag. Även om det är olyckligt så är det naturligt att dataskyddsarbetet till viss del gått i stå under den period då den typen av kompetens saknats i organisationen. Dataskyddsombudet vill ändå lyfta att verksamheten även i avsaknad av särskild dataskyddskompetens har genomfört en konsekvensbedömning under hösten med mycket hög kvalitet. Även om det ändå återstår visst arbete med att omhänderta dataskyddsombudets samtliga rekommendationer avseende den bedömningen.

Så vitt dataskyddsombudet förstår har bolaget nu också gjort klart med en nyrekrytering till dataskyddsorganisationen, vilket så klart är positivt. Svårigheterna att rekrytera visar på riskerna med att fastna i ett personberoende, samtidigt har dataskyddsombudet viss förståelse för att det i avsaknad av en dedikerad resurs är svårt att driva dataskyddsarbetet på ett ändamålsenligt sätt. Dataskyddsombudet är också medveten om att bolaget verkligen ansträngt sig för att hitta rätt person med hög kompetens. Det finns fortfarande en hel del saker som bolaget behöver ta tag i och slutföra när ny dataskyddsspecialist är på plats. Framför allt handlar det om att säkerställa en ändamålsenlig dataskyddsorganisation, att se till att dataskyddsarbetet får genomslag i hela verksamheten, att omhänderta dataskyddsombudets rekommendationer kring behandlingsregister, samt att färdigställa de konsekvensbedömningar som bolaget nästan tagit i mål, men inte riktigt nått ända fram i. Avslutningsvis vill dataskyddsombudet särskilt lyfta att även om bolagets svar på dataskyddsombudets kontrollfrågor indikerar att det kvarstår brister i organisationens dataskyddsarbete, så är dataskyddsombudets samlade bedömning att GS är på rätt väg och att verksamheten tagit stora steg framåt de senaste två åren.

4 Granskning av dataskyddsarbetet 2025

4.1 Övergripande kontroll 2025

Under 2025 har dataskyddsombudet kontrollerat verksamhetens dataskyddsarbete utifrån tio kontrollpunkter. Kontrollen har genomförts genom en enkät. Enkäten är avsedd att spänna över de viktigaste delarna inom dataskyddsarbetet för att på så sätt fånga in en större bredd av frågor. Metoden syftar till att få till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

Enkäten består av tio kontrollpunkter där varje punkt innehåller ett antal delfrågor utformade som påståenden. Verksamheten ska i svaret uppskatta hur väl påståendet stämmer in på verksamheten utifrån en fyrgradig skala. Nytt för i år är att verksamheten även ska motivera sina svar i vissa fall. Syftet med detta är att öka dataskyddsombudets möjlighet till insyn. Om något saknas i verksamheternas dokumenterade arbetssätt behöver det framgå så att det blir tydligt för dataskyddsombudet och för verksamheten var bristerna finns i det systematiska arbetet, så att det kan åtgärdas.

4.1.1 Ett riskbaserat arbetssätt

I kontrollarbetet används en modell som består av fyra kategorier, vilka representerar fyra olika risknivåer. Verksamheten får utifrån sina svar ett värde som visar vilken risknivå verksamheten befinner sig på inom respektive kontrollpunkt. Genom att arbeta med risknivåer möjliggörs ett riskbaserat arbetssätt för både verksamhet och dataskyddsombud, då resultaten ger en bild av vad verksamheten behöver prioritera i dataskyddsarbetet framåt.

Risknivå	Beskrivning	Färgkod
Nivå 1	Höga risker identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten.	
Nivå 2	Risker identifierade som bedöms vara omfattande och/eller kräver omgående åtgärder.	
Nivå 3	Risker identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.	
Nivå 4	Inga direkta risker av betydelse identifierade. Indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete.	

4.1.2 Verksamhetens resultat

Verksamhetens resultat illustreras genom diagram, se bilaga 2. Diagrammet visar vilken risknivå verksamheten befinner sig inom för respektive kontrollpunkt, och utgår enbart från verksamhetens egna svar på frågorna i enkäten.

Dataskyddsombudet gör i årsrapporten ingen bedömning eller analys av resultatet som helhet, utan kommenterar företrädesvis resultatet för de kontrollpunkter som varit rekommenderade fokusområden för 2025 i samband med uppföljningen samt de delar som uppenbart avviker från dataskyddsombudets bedömning.

Resultatet av kontrollen kommer, tillsammans med de rekommenderade fokusområdena för 2026, utgöra grunden för dataskyddsombudets arbete med verksamheten under kommande år.

Särskilda iakttagelser kopplat till verksamhetens resultat

Bolaget har i många kontrollfrågor skattat sitt eget resultat lågt. Att resultatet är lågt är naturligtvis inte bra, samtidigt finner dataskyddsombudet det positivt att verksamheten inte på något sätt försöker skönmåla. Tanken med kontrollen är att dataskyddsombudet ska få rättvisande information om verksamhetens dataskyddsarbete, och det bedömer dataskyddsombudet att verksamheten har bidragit med. Till exempel har bolaget skattat att förutsättningarna på pappret finns för organisationen av dataskyddsarbetet, men att genomslaget i praktiken inte fått effekt i organisationen och att det finns ett stort mått av personberoende. Vad gäller konsekvensbedömningar har verksamheten skattat det egna arbetet högt, vilket också är dataskyddsombudets bedömning, då bolaget gjort ett omfattande arbete avseende just den kontrollpunkten. Vad gäller bolagets skattning av kontrollpunkt 10, de registrerades rättigheter, så framgår det efter avstämning med verksamheten att bristerna i hantering av de registrerades rättigheter har åtgärdats från det att bolaget inkom med sina svar på kontrollfrågorna och upprättandet av denna årsrapport. Dataskyddsombudet ser mycket positivt på att bolaget själva, med stöd i dataskyddsombudets kontrollfrågor, identifierat och åtgärdat brister i det arbetet.

4.1.3 Uppföljning av verksamhetens arbete med rekommenderade fokusområden 2025

Dataskyddsombudet har följt upp hur verksamheten arbetat med de fokusområden som rekommenderades för 2025.

Fokusområde 1: Dataskyddsorganisation

Verksamheten gavs följande rekommendationer:

Dataskyddsombudet rekommenderar att bolaget lägger fokus på att se över kontrollpunkten i sin helhet för att säkerställa en ändamålsenlig och adekvat resurssatt dataskyddsorganisation med tydliga mandat att driva dataskyddsfrågor i verksamheten. Fokusområdet kvarstår från 2023, bolaget har kommit en bra bit på

vägen, men dataskyddsombudet bedömer att GS fortsatt behöver fokusera på frågan under 2025.

Som svar på dataskyddsombudets- kontrollfrågor och uppföljning har bolaget angett följande:

Bolaget har utsedd dataskyddskontakt (DSK) och flera dataskyddsamordnare. Respektive roll är dokumenterad och förankrad i bolagsledningen. Det finns en fastställd dataskyddsorganisation, som inte har blivit etablerad fullt ut. Mycket av dataskyddsarbetet inom bolaget har varit på enstaka personer, vilket skapat ett personberoende. En del av verksamheten vet att det varit en specifik person som arbetat med dataskydd heltid. Men det har inte varit tydligt för hela organisationen. Det är inte tydligt hur mycket tid som ska vikas till dataskyddsarbetet. Det finns en plan för dataskyddsarbetet, som har antagits i bolagsledningen, men planen följs inte upp regelbundet eller återrapporteras till högsta ledningen. Vad gäller involvering av dataskyddsombudet så finns det ett dokumenterat arbetssätt inom organisationen, men trots det involveras inte dataskyddsombudet i samtliga frågor som rör dataskydd

Avslutningsvis uppger bolaget att GS haft problem att rekrytera kompetens till dataskyddsorganisationen, men att ny resurs kommer finnas på plats i januari 2026 och att bolaget har för avsikt att följa dataskyddsombudets rekommendation och säkerställa en ändamålsenlig och adekvat resurssatt dataskyddsorganisation med tydliga mandat att driva dataskyddsfrågor i verksamheten.

Kommentarer och rekommendationer:

Det är viktigt att den dataskyddsorganisation som finns inte bara blir en pappersprodukt. Bolaget behöver därför verka för att dataskyddsarbetet får genomslag i verksamheten och inte bara vilar på en eller några få personer. Ett led i detta är att det blir tydligt vem verksamheten kan vända sig till och hur ansvaret i övrigt ska vara fördelat i organisationen, till exempel vilket ansvar som vilar på chefer. Det är också viktigt att den plan som faktiskt finns för hur arbetet ska bedrivas följs upp årligen och justeras efter behov. Dataskyddsombudet är medveten om att bolaget under längre tid försökt rekrytera nödvändig kompetens till dataskyddsorganisationen. Dataskyddskompetens är erkänt svårrekryterad på grund av ett stort behov och litet utbud. Eftersom dataskyddsombudet vet att bolaget aktivt jobbar med frågan, i vissa fall också rådgjort med dataskyddsombudet, så lämnas ingen annan rekommendation än att fortsätta verka för att säkerställa en ändamålsenlig dataskyddsorganisation. I dialog med verksamheten har också framkommit att bolaget lyckats rekrytera en dataskyddsspecialist som påbörjar sin anställning i januari 2026. När denne är på plats bör bolaget fortsätta verka för att fastställa formerna för dataskyddsorganisationens arbete.

Fokusområde 2: Register över personuppgiftsbehandlingar

Verksamheten gavs följande rekommendationer:

GS rekommenderas att göra en översyn av hur behandlingar dokumenterats i bolagets behandlingsregister enligt artikel 30 i GDPR med utgångspunkt i de

vägledning som dataskyddsombudet lämnat i den staden-gemensamma granskningsrapporten avseende 2024 års fördjupade kontroll.

Som svar på dataskyddsombudets uppföljning har bolaget angett följande:

Göteborgs Spårvägar har för avsikt att följa dataskyddsombudets rekommendation genom att göra en översyn av hur behandlingar dokumenterats i bolagets behandlingsregister enligt artikel 30 i GDPR med utgångspunkt i de vägledning som dataskyddsombudet lämnat i den staden-gemensamma granskningsrapporten avseende 2024 års fördjupade kontroll. Merparten av behandlingarna är inlagda i behandlingsregistret men informationen är inte komplett, vidare saknar bolaget arbetssätt med tydligt definierade roller och ansvarsområden, för att kontinuerligt uppdatera registret med behandlingar som tillkommit eller förändrats.

Kommentarer och rekommendationer:

Att bolaget inte kunnat omhänderta dataskyddsombudets rekommendation får anses vara följdriktigt av att det inte funnits någon dedikerad dataskyddsspecialist på plats. Med det sagt så behöver bolaget under 2026 genomföra en översyn av registret för att säkerställa att all information finns med och att den följer de rekommendationer som dataskyddsombudet lämnat. Bolaget behöver också säkerställa att det finns rutiner och arbetssätt som säkerställer att registret hålls uppdaterat. Fokusområdet kommer kvarstå under 2026 och bolaget bör prioritera arbetet när ny dataskyddsspecialist finns på plats.

5 Rekommenderade fokusområden 2026

Dataskyddsombudet rekommenderar, utifrån gjorda iakttagelser och resultaten av uppföljningen, verksamheten att under 2026 fortsätta prioritera arbetet med de kontrollpunkter som rekommenderas för 2025. 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 2026.

Förvaltningen/bolaget rekommenderas under 2026 prioritera följande delar av dataskyddsarbetet:

- Kontrollpunkt 1: Dataskyddsorganisation

Dataskyddsombudet rekommenderar att bolaget lägger fokus på att se över kontrollpunkten i sin helhet för att säkerställa en ändamålsenlig och adekvat resurssatt dataskyddsorganisation med tydliga mandat att driva dataskyddsfrågor i verksamheten. Fokusområdet kvarstår från 2023. Dataskyddsombudet bedömer att GS fortsatt behöver fokusera på frågan under 2026.

- Kontrollpunkt 2: Register över personuppgiftsbehandlingar

GS rekommenderas att göra en översyn av hur behandlingar dokumenterats i bolagets behandlingsregister enligt artikel 30 i GDPR med utgångspunkt i den vägledning som dataskyddsombudet lämnat. Fokusområdet kvarstår från 2024.

6 Bilagor

Bilaga 1: Reviderade kontrollpunkter

Bilaga 2: Verksamhetens resultat från den övergripande kontrollen 2025

Bilaga 1: Reviderade kontrollpunkter

Kontrollpunkter 2025	**Kommentar**
Kontrollpunkt 1: Dataskyddsorganisation och övergripande styrning i dataskyddsarbetet	Ersätter de tidigare kontrollpunkterna *Dataskyddsorganisation* och *Övergripande styrning i dataskyddsarbetet*.
Kontrollpunkt 2: Register över personuppgiftsbehandlingar	Namn på kontrollpunkt oförändrat.
Kontrollpunkt 3: Hantering av personuppgiftsincidenter	Ersätter den tidigare kontrollpunkten *Personuppgiftsincidenter*.
Kontrollpunkt 4: Utbildning	Namn på kontrollpunkt oförändrat.
Kontrollpunkt 5: Information till registrerade	Ersätter den tidigare kontrollpunkten *Informationsplikt*.
Kontrollpunkt 6: Konsekvensbedömning/samråd	Namn på kontrollpunkt oförändrat.
Kontrollpunkt 7: Informationshantering	Ersätter den tidigare kontrollpunkten *E-post och dokumenthantering*, samt delar av kontrollpunkterna *IT-projekt och upphandling* och *IT-system och digitala verktyg.*
Kontrollpunkt 8: Säkerhet	Ersätter delar av de tidigare kontrollpunkterna *IT-projekt och upphandling* och *IT-system och digitala verktyg.*
Kontrollpunkt 9: Biträdesavtal och andra överenskommelser	Namn på kontrollpunkt oförändrat. Kompletteras med delar från den tidigare kontrollpunkten *IT-projekt och upphandling*.
Kontrollpunkt 10: Hantering av registrerades rättigheter	Namn på kontrollpunkt oförändrat.

Bilaga 2: Verksamhetens resultat 2025