Göteborgs Stad

Årsrapport för dataskyddsarbetet 2025

Renova AB

2025-12-19

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

Dataskyddsombudet har haft en aktivt rådgivande roll i arbetet att genomföra delar av bolagets arbete under 2025. Dataskyddsombudet har involverats i regelbundna avstämningsmöten och konsulterats av verksamheten i olika frågor. Dataskyddsombudet uppfattning är att bolaget arbetar målmedvetet med frågor om integritet och dataskydd och är i process att hantera kvarstående förbättringsåtgärder. Verksamheten har god självinsikt och ser fortsatt behov av att förstärka utbildningsinsatser och mognadsgraden i dataskyddsfrågor för ett tydligare genomslag i organisationen som helhet.

Rekommendationen är att bolaget fullföljer färdigställandet av förra årets kontrollpunkter och fokusområden. Utöver nödvändiga kompletteringar med att färdigställa bolagets behandlingsregister rekommenderas bolaget fortsatt prioritera konsekvensbedömningsarbetet under 2026 samt vid genomförandet även då säkerställa tid och resurser som krävs liksom fortsatt följa rutinen för att inhämta dataskyddsombudets synpunkter. Utifrån årets övergripande kontroll och bolagets skattning är en utvidgning av fokusområden inte aktuell i nuläget eftersom ett komplett behandlingsregister är ett centralt och viktigt verktyg för ett fungerande dataskyddsarbete. Därjämte i arbetet med att färdigställa behandlingsregistret och genomföra konsekvensbedömningar ingår att identifiera tekniska och organisatoriska säkerhetsåtgärder liksom biträdesrelationer.

Dataskyddsombudet sammantagna uppfattning är att bolaget har god kompetens inom organisationen och att det finns goda förutsättningar att utveckla dataskyddsarbetet. Det är viktigt att bolagsledningen fortsätter att tydligt prioritera integritets- och dataskyddsfrågor och därmed skapa och upprätthålla ett långsiktigt och uthålligt engagemang i hela verksamheten.

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

Bolagets resultat gällande kontrollpunkterna 6, *Konsekvensbedömning/samråd*, 8 *Säkerhet* och 9 *Biträdesavtal och andra överenskommelser* indikerar att det inom kontrollpunkterna föreligger risker som behöver åtgärdas.

Alla kontrollpunkter hänger samman och behandlingsregistret är ett centralt och viktigt verktyg för ett fungerande dataskyddsarbete. I arbetet med att färdigställa behandlingsregistret och genomföra konsekvensbedömningar ingår att identifiera tekniska och organisatoriska säkerhetsåtgärder liksom biträdesrelationer.

Dataskyddsombudets bedömning är därför att en utvidgning av fokusområden inte är aktuell i nuläget. Rekommendationen är att bolaget fullföljer färdigställandet av förra årets fokusområden.

4.2 Uppföljning av lämnade rekommendationer

4.2.1 Uppföljning av verksamhetens arbete med rekommenderade fokusområden 2025

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

Fokusområde 1: Register över personuppgiftsbehandlingar (Kontrollpunkt 2)

Verksamheten gavs följande rekommendationer:

Bolaget rekommenderades kartlägga och komplettera behandlingsregistret enligt artikel 30 i GDPR. Ta del av och beakta rekommendationerna som framgår i den fördjupade kontrollen men även i den generella granskningsrapporten som

vägledning. Säkerställa förbättringsåtgärderna och inkorporera ett arbetssätt för att hålla registret uppdaterat och korrekt.

Kommentarer och rekommendationer:

Bolaget uppger att inför överföringen av behandlingsregistret till ett nytt systemverktyg, ISDB, gjordes ett arbete med att kartlägga fler behandlingar och komplettera befintliga. Bolaget har beaktat den vägledande generella granskningsrapporten liksom kompletterande förslag avseende de staden gemensamma behandlingarna som skickats ut.

Bolaget uppger vidare att åtgärder för att se över och uppdatera behandlingsregistret minst 1 gång årligen finns inlagda i bolagets årshjul. Det finns dock inget dokumenterat arbetssätt för hur detta ska gå till, utan det är Informationssäkerhetsansvarig i bolaget som ansvarar för att hålla behandlingsregistret uppdaterat och korrekt. Arbetet med behandlingsregistret pågår och planen framåt är att även kartlägga vilka av verksamhetens system som innehåller artikel 30 information för att få bättre kontroll över vilka uppgifter som hanteras och varför.

Bolagets behandlingsregister har även varit föremål för dataskyddsombudets fördjupade kontroll med tillhörande och mera specifika rekommendationer. Utifrån bolagets svar framgår att rekommendationerna har beaktats i möjligaste mån. Flertal kolumner har justerats som tillsammans med de staden gemensamma behandlingsförslag har bidragit till ett mer heltäckande behandlingsregister. Behandlingsregistret är dock inte komplett och det uppges bero på att information från verksamheten saknas. Enligt bolaget uppges den största utmaningen med behandlingsregister och möjligheterna att hålla det uppdaterat, hänga ihop med verksamhetens mognadsgrad. Verksamhetens kunskap behöver höjas ytterligare innan de blir tillräckligt självgående för att identifiera och rapportera att nya behandlingar påbörjas eller att befintliga behöver uppdateras. Enligt uppgift har behandlingsregistret kompletterats utifrån de förutsättningar som finns i verksamheten och att det är ett ständigt pågående arbete.

Dataskyddsombudet har inte tagit del av bolagets behandlingsregister men ser det som positivt att bolaget har aktivt prioriterat och arbetat med rekommendationerna kopplade till behandlingsregistret.

Eftersom uppföljningen visar att verksamheten fortfarande har förbättringsområden inom denna kontroll är rekommendationen att fortsatt prioritera frågan och följdriktigt säkerställa att bolagets behandlingsregister är komplett och uppfyller kraven i enlighet med artikel 30 i GDPR.

Fortsatt uppföljning kommer därför att ske under 2026.

Fokusområde 2: Utbildning (Kontrollpunkt 4)

Verksamheten gavs följande rekommendationer:

Bolaget rekommenderades öka och dokumentera den generella kunskapsnivån inom dataskydd hos medarbetare som inkluderat involverad hantering av behandlingsregister.

Kommentarer och rekommendationer

Enligt bolagets uppgift pågår olika utbildningsinsatser kontinuerligt. Dels ett antal utbildningar kopplade till både informationssäkerhet och GDPR i bolagets Kompetensportal, dels även utbildningar på grundnivå och fortsättningskurser. Dessa kurser uppges ingå i program för nyanställda och nya chefer samt är även tillgängliga för alla medarbetare oavsett befattning. Bolaget uppges ha möjlighet att få ut utbildningsstatistik på hur många som anmält sig och genomfört de olika utbildningarna. Bolaget planer också att genomföra behovsanpassade riktade utbildningsinsatser för olika stödfunktioner/enheter. Därutöver har utbildning i GDPR och Informationssäkerhet genomförts på ett antal APT:er där bolaget även tagit upp vikten av behandlingsregister och verksamhetens ansvar i detta. Under året har bolaget uppmärksammat även Cybersäkerhetsmånaden genom bland annat informationsblad på ett antal utvalda anläggningar samt information på bolagets Intranät med syfte att höja medvetenhet och öka förståelsen för dataskyddsfrågor.

Dataskyddsombudet ser positivt på att bolaget har vidtagit aktuella åtgärder. Förutsatt att identifierade riktade utbildningsinsatser genomförs liksom övriga kontinuerliga utbildningar framgent kommer kontrollpunkten att ingå i det löpande uppföljningsarbetet och inte utgöra ett rekommenderat fokusområde 2026.

Fokusområde 3: Konsekvensbedömningar/samråd (Kontrollpunkt 6)

Verksamheten gavs följande rekommendationer:

Bolaget rekommenderades identifiera befintliga högriskbehandlingar och ta fram dokumenterade arbetssätt för att hantera riskerna liksom uppföljningen.

Kommentarer och rekommendationer:

Under året har bolaget identifierat och genomfört ett par konsekvensbedömningar avseende bakgrundskontroller och drogtester samt följt rutinen att involvera dataskyddsombudet. Enligt uppgift har bolaget även påbörjat en konsekvensbedömning för schemaläggning, tid och bemanning samt identifierat behov av att genomföra en konsekvensbedömning kopplat till arbetsmiljö och då specifikt hantering av incidenter och tillbud (IA).

Det uppges även att ett arbete pågår med att ta fram rutin för konsekvensbedömningar där det framgår varför det behöver göras, när det ska göras, vem som ska kontaktas samt vems ansvar det är. Planen framåt är att identifiera fler högriskbehandlingar och skapa en prioriteringsordning för dessa.

Dataskyddsombudet ser positivt på bolagets insikter och planerade åtgärder. Mot bakgrund av att konsekvensbedömningsarbetet inte är engångsaktivitet utan ett dokumentationsverktyg för verksamheten att förstå integritetsriskerna och kontinuerligt arbeta med att vidta nödvändiga riskreducerande skyddsåtgärder

kvarstår rekommenderat fokusområde och kommer därför att följas upp under 2026.

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.

Bolaget rekommenderas under 2026 prioritera följande delar av dataskyddsarbetet:

- Kontrollpunkt 2: Register för personuppgiftsbehandlingar

Komplettera och dokumentera personuppgiftsbehandlingar enligt artikel 30 i GDPR. Fortsatt beakta rekommendationerna som framgår i den fördjupade kontrollen men även i den generella granskningsrapporten som vägledning. Säkerställa förbättringsåtgärderna och inkorporera ett arbetssätt för att hålla registret uppdaterat och korrekt.

- Kontrollpunkt 6: Konsekvensbedömning/samråd

Ta fram plan för behandlingar som kräver konsekvensbedömning. Säkerställa tid och resurser som krävs för att genomföra konsekvensbedömingsarbetet, säkerställa förbättringsåtgärderna. Därtill fortsatt följa rutinen för att inhämta dataskyddsombudets synpunkter.

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