



Årsrapport för dataskyddsarbetet 2025

Gryaab AB

2025-12-19

Innehåll

1	Inledning	3
1.1	Göteborgs Stads dataskyddsombud.....	3
1.2	Ändringar i kontrollarbetet 2025.....	3
2	Stadenövergripande iakttagelser 2025.....	4
2.1	Arbete med digitalisering och AI kräver dataskyddsresurser	4
2.2	Årets incidenter visar på betydelsen av grundläggande dataskyddsarbete.....	4
3	Verksamhetsspecifika iakttagelser 2025.....	6
3.1	Verksamhetens dataskyddsarbete	6
4	Granskning av dataskyddsarbetet 2025.....	7
4.1	Övergripande kontroll 2025	7
4.1.1	Ett riskbaserat arbetssätt	7
4.1.2	Verksamhetens resultat.....	8
4.2	Uppföljning av lämnade rekommendationer.....	9
4.2.1	Uppföljning av verksamhetens arbete med rekommenderade fokusområden 2025	9
5	Rekommenderade fokusområden 2026	11
6	Bilagor	13
	Bilaga 1: Reviderade kontrollpunkter	14
	Bilaga 2: Verksamhetens resultat 2025	15

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 följderna 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 oftast skriftligen 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 dataskyddsombudets rekommendationer. Tempot i arbetet med att uppdatera behandlingsregistret behöver dock öka. Bolaget behöver också 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. Därtill och utifrån bolagets skattning, trots att alla dataskyddspunkter hänger samman, är det av särskilt vikt att under 2026 även fokusera på information till registrerade samt hantering av registrerades rättigheter.

Följdriktigt är också viktigt att bolagsledningen fortsätter att tydligt prioritera frågor kopplat till integritet och dataskydd. Ett långsiktigt och uthålligt engagemang för integritet och dataskyddsfrågor i hela verksamheten är viktiga förutsättningar för bolagets fortsatta utveckling.

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.

Riskenivå	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

Kontrollpunkt 5: Information till registrerade

Bolagets resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas.

Informationsplikten är långtgående och omfattar mer än den information som ges på bolagets hemsida. För att informationsplikten ska anses vara uppfylld finns det krav på såväl när informationen ska lämnas, vilken information som lämnas och hur den lämnas. Informationen ska vara lättillgänglig oavsett i vilken del av verksamheten den registrerades personuppgifter behandlas.

Personuppgiftsansvariga ska även informera om alla personuppgiftsbehandlingar som genomförs.

Eftersom informationen som lämnas till registrerade ska överensstämma med behandlingregistret är rekommendationen att bolaget intensifierar arbetet med att uppdatera all information. Därtill ta fram dokumenterade arbetssätt för att kontinuerligt se över och uppdatera integritetsinformationen.

Kontrollpunkt 10: Hantering av registrerades rättigheter

En förutsättning för att hantera registrerades rättigheter är att bolaget har rutiner på plats för att hantera begäranden om att utöva dessa rättigheter när någon begär det.

Parallellt med uppdatering av all information rekommenderas bolaget dokumentera och-/eller uppdatera befintligt arbetssätt för att hantera registrerades rättigheter.

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 att kartlägga och dokumentera personuppgiftsbehandlingar enligt artikel 30 i GDPR. Ta del av den generella granskningsrapporten från dataskyddsombudets fördjupade kontroll och beakta rekommendationerna som framgår däri vid arbete med behandlingsregistret.

Kommentarer och rekommendationer:

Bolaget uppger att en rutin för hantering av behandlingsregister finns framtagen och ligger för godkännande av bolagets vd. Bolaget har också tagit del av den generella granskningsrapporten från dataskyddsombudets fördjupade kontroll men ännu inte uppdaterat sitt behandlingsregister. Detta uppges bero på att bolaget har avvaktat systembyte och dataskyddsfunktionens förslag på behandlingsregister gällande stadengemensamma behandlingar. Vidare uppges att uppdateringsarbetet kommer att prioriteras under hösten och våren 2026.

Dataskyddsombudet har inte tagit del av bolagets rutin. Eftersom arbetet med att uppdatera och komplettera behandlingsregister kvarstår kommer uppföljning därför att ske igen under 2026.

Fokusområde 2: E-post och dokumenthantering

Verksamheten gavs följande rekommendationer:

Bolaget rekommenderades säkerställa förbättringsåtgärderna och inkorporera ett arbetssätt för e-post och dokumenthantering.

Kommentarer och rekommendationer

Enligt uppgift har bolaget genomfört flera utbildningsinsatser kring informationssäkerhet och hantering av e-post. Bolaget har även uppdaterat sin dokumenthanteringsplan med gallringsrutiner. Informationsklassningsarbetet har påbörjats och bolaget uppger att kvarstående åtgärder kommer att vidtas beroende på vad som framkommer i klassningen.

Uppföljningen visar att verksamheten fortfarande har förbättringsområden inom denna kontroll. Dataskyddsombudet rekommenderar att fullfölja informationsklassningsarbetet och vidta identifierade förbättringsåtgärder. Dokumentera arbetssätt för att kontrollera och följa upp att personuppgifter lagras enligt fastställda tidsfrister. Dokumenterade arbetssätt för att systematiskt kunna följa upp och kontrollera att användningen av medlen följer interna riktlinjer.

Uppföljning kommer därför att ske igen under 2026.

Fokusområde 3: Konsekvensbedömning/samråd (Kontrollpunkt 6)

Verksamheten gavs följande rekommendationer:

Bolaget rekommenderades säkerställa förbättringsåtgärderna och inkorporera ett arbetssätt för att inhämta dataskyddsombudets synpunkter för pågående liksom framtida konsekvensbedömningar.

Kommentarer och rekommendationer:

Bolaget uppger att en rutin för hantering av konsekvensbedömningar/samråd har tagits fram och ligger hos vd för fastställande. Av rutinen framgår när dataskyddsombudets synpunkter ska inhämtas och att dataskyddsombudet har involverats i framtagandet av rutinen.

Vidare uppges att tröskelanalyser/konsekvensbedömningar på nya behandlingar har prioriterats. Bolaget kommer att ta fram en prioriteringsordning utifrån en riskanalys för bolagets befintliga behandlingar och arbeta utifrån denna. Arbetet planeras under hösten 2025.

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 är rekommendationen att bolaget mera skyndsamt genomför och bedömer högriskbehandlingar som saknas utifrån risker för de registrerade. Förutom att säkerställa tid och resurser som krävs vid genomförandet är det viktigt att fortsatt följa rutinen för att inhämta dataskyddsombudets synpunkter.

Rekommenderat fokusområde kvarstår 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. Såväl verksamheten som dataskyddsombudet har under avstämningsarbetet tillsammans identifierat ett par kontrollpunkter till som verksamheten rekommenderas arbeta med parallellt under det kommande året.

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 över personuppgiftsbehandlingar

Kartlägga och dokumentera personuppgiftsbehandlingar enligt artikel 30 i GDPR. Beakta rekommendationerna som framgår i den generella granskningsrapporten från dataskyddsombudets fördjupade kontroll.

- Kontrollpunkt 5: Information till registrerade

Uppdatera all information till de registrerade och säkerställa att informationen uppfyller de innehållsmässiga och formmässiga kraven.

Tillse att den information som finns i verksamhetens behandlingsregister överensstämmer med den information som lämnas till de registrerade.

Ta fram dokumenterade arbetssätt för att kontinuerligt se över och uppdatera integritetsinformationen.

- Kontrollpunkt 6: Konsekvensbedömning/samråd

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

- Kontrollpunkt 7: Informationshantering

Fullfölja informationsklassningsarbetet och vidta identifierade förbättringsåtgärder. Dokumentera arbetssätt för att kontrollera och följa upp att personuppgifter lagras enligt fastställda tidsfrister. Dokumentera arbetssätt för att systematiskt kunna följa upp och kontrollera att användningen av medlen följer interna riktlinjer.

- Kontrollpunkt 10: Hantering av registrerades rättigheter

Dokumentera och-/eller uppdatera befintligt arbetssätt för att hantera registrerades rättigheter.

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

Bilaga 2: Verksamhetens resultat 2025

