



Årsrapport för dataskyddsarbetet 2025

Higab 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.....	8
4.2.1	Uppföljning av verksamhetens arbete med rekommenderade fokusområden 2025	8
5	Rekommenderade fokusområden 2026	11
6	Bilagor	12
	Bilaga 1: Reviderade kontrollpunkter	13
	Bilaga 2: Verksamhetens resultat 2025	14

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 avstämningsmöten och konsulterats av verksamheten i frågor hänförliga till både tröskelanalyser och konsekvensbedömningar. Förutom färdigställandet av det uppdaterade behandlingsregistret bör bolaget fortsatt och generellt prioritera konsekvensbedömningsarbetet under 2026 samt vid genomförandet säkerställa tid och resurser som krävs liksom hittills följa rutinen för att inhämta dataskyddsombudets synpunkter. Dataskyddsombudet noterar att bolaget har skickat in en konsekvensbedömning i november och har aktiverat Copilot Chat innan dataskyddsombudets utlåtande. Dataskyddsombudet vill framföra att detta förfarande inte är att likställa med att bolaget har involverat dataskyddsombudet i arbetet utifrån de krav som ställs enligt GDPR. Bolaget har därför fått frågan att skicka över beslutsunderlag till dataskyddsombudet för påsyn. Bolaget är i process att hantera dataskyddsombudets begäran om beslutsunderlag liksom i övrigt lämnade rekommendationer. Det 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.

Dataskyddsombudets samlade bedömning vad avser efterlevnad av dataskyddsförordningen är att de goda förutsättningar som för närvarande finns också bibehålls och utvecklas.

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 10: Hantering av registrerades rättigheter

Bolagets resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas. Hantering av registrerades rättigheter avser verksamhetens förutsättningar och rutiner för att hantera de registrerades rättigheter, till exempel begäran om registerutdrag, rättelse eller radering.

Bolaget i rollen som personuppgiftsansvarig har ett ansvar för att följa GDPR men också kunna visa att reglerna följs genom att ha rutiner på plats för att hantera begäranden om någon begär och vill utöva dessa rättigheter.

Bolaget uppger att arbetssättet inte är skriftligt dokumenterat, men att muntlig rutin finns. I linje med principen om ansvarsskyldighet är rekommendationen att upprätta interna styrande dokument.

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.

Kommentarer och rekommendationer:

Bolaget uppger att en översyn över samtliga behandlingar har gjorts innan migrering av datainformation till det nya systemet ISDB (iFacts). Enligt uppgift gjordes ändringar utifrån infallsvinkel att se en behandling som en del av en process än som en ensam händelse. Vidare uppges att bolaget kommer att beakta och komplettera sitt behandlingsregister utifrån mall/handledning från dataskyddsfunktionens stadengemensamma behandlingsregister som är på gång.

Dataskyddsombudet har inte tagit del bolagets behandlingsregister eftersom en del av arbetet med kompletterande behandlingar kvarstår. Ett råd är att parallellt tillse att den information som finns i verksamhetens behandlingsregister överensstämmer med den information som lämnas till de registrerade.

Fortsatt uppföljning kommer därför att ske under 2026.

Fokusområde 2: Konsekvensbedömning/samråd (Kontrollpunkt 6)

Verksamheten gavs följande rekommendationer:

Bolaget rekommenderades inhämta dataskyddsombudets synpunkter för pågående liksom framtida konsekvensbedömningar. Säkerställa förbättringsåtgärderna och inkorporera ett arbetssätt för att och i de fall där så krävs även inhämta de registrerades synpunkter.

Kommentarer och rekommendationer:

Enligt bolagets uppgift har bolaget ett arbetssätt att vid genomförandet av konsekvensbedömningar involvera dataskyddsombudet och att det har också gjorts i alla de konsekvensbedömningar som hittills är gjorda. Vidare uppges att eftersom arbetet med konsekvensbedömningarna mycket sällan sker isolerat utan som en del i bolagets digitala verksamhetsutvecklingsprojekt, så är de vars personuppgifter förekommer mest - dvs medarbetarna – en del i projektgrupperna och används som bollplank även i bedömningarna.

Dataskyddsombudet har involverats både i tröskelanalysarbetet och konsekvensbedömningsarbetet. Bolaget är i process att omhänderta lämnade synpunkter och rekommendationer och 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 fortsätter på den inslagna linjen, 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.

Dataskyddsombudet har noterat bolagets kommentar när det gäller att inhämta synpunkter från registrerade och lämnar ett förtydligande. Oavsett om referensgrupper eller användargrupper i form av medarbetare deltar i konsekvensbedömningsarbetet också tillfrågas bör bolaget tillse separat dokumentation över synpunkterna. Om det rör behandlingar som enligt bolagets uppgift oftast omfattar just medarbetare är det lämpligt att synpunkter inhämtas från skyddsombud eller de arbetstagarorganisationer som finns representerade på arbetsplatsen.

Uppföljningen visar att verksamheten har vidtagit åtgärder i enlighet med samtliga rekommendationer. Fortsatt uppföljning sker i det löpande arbetet under 2026.

5 Rekommenderade fokusområden 2026

Dataskyddsombudet rekommenderar, utifrån gjorda iakttagelser och resultaten av uppföljningen, verksamheten att under 2026 fortsätta prioritera arbetet med en av kontrollpunkterna som rekommenderade 2025. Såväl verksamheten som dataskyddsombudet har under avstämningsarbetet med årsrapporten tillsammans identifierat ännu en kontrollpunkt 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

Komplettera och dokumentera personuppgiftsbehandlingar enligt artikel 30 i GDPR. Tillse att den information som finns i verksamhetens behandlingsregister överensstämmer med den information som lämnas till de registrerade.

- Kontrollpunkt 10: Hantering av registrerades rättigheter

Upprätta interna styrande dokument gällande hantering av 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

