Stockholms stad

Dataskyddsombudets årsrapport 2025

S:t Erik Markutveckling

Dataskyddsombudets årsrapport 2025
Januari 2026
Dnr: STEM 2026/20
Kontaktperson: Micaela Caldegren
Konsult: Jessica Hillergård

1 Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

Den personuppgiftsansvariga behöver ha god insikt i dataskyddsarbetet. Ett sätt att hålla sig informerad om risker och trender är den här årsrapporten.

Dataskyddsåret 2025 har varit fyllt av utmaningar men också möjligheter. En av nyheterna är att IMY, Integritetsskyddsmyndigheten, nu vill fokusera mer på vägledning än bestraffning. Det var med stor glädje vi mottog tydlig vägledning i både hur konsekvensbedömningar ska vara utformade och hur arbetet med AI-förordningen ska gå till.

En omvärldsbevakning från mig som DSO, är att tillsynsmyndigheten vill lägga mer fokus under 2026 på riskarbete inom dataskydd. Några av de riskområden som jag vill belysa i min årsrapport är:

- Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (STEM:s) objektförvaltning.
- Ny teknik, t.ex. behandling av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation.
- Tredjelandsöverföringar
- Lagringsytor utan kontroll

Vi står inför en tid av mycket osäkerheter där vem som är allierad och riskerna inom cybersäkerhet och informationssäkerhet förändras fort. Min uppgift som DSO är att se till att de registredes skyddas på ett adekvat och tryggt sätt.

Jag ber också att få tacka för förtroendet jag fått att vara er DSO sedan 2020. Jag önskar DSO:erna från Serviceförvaltningen lycka till och att vi får ett lagom spännande och intressant dataskyddsår framför oss!

Jessica Hillergård

Dataskyddsombud

Innehåll

2 Inledning

2.1 Bakgrund

Dataskyddsförordningen, GDPR, trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

Enligt dataskyddsförordningen är varje nämnd och bolagsstyrelse inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnd eller styrelse behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett dataskyddsombud, DSO. Denna roll har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är således ett medel för personuppgiftsansvarig att ta emot de råd och rekommendationer som dataskyddsombudet är skyldig att ge till ansvarig enligt dataskyddsförordningen. I rapporten får personuppgiftsansvarig insyn i vad dataskyddsombudets granskningar visat av verksamheten och status avseende integritet och dataskydd. Årsrapporten syftar till att personuppgiftsansvarig ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd eller styrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att personuppgiftsansvarig ska kunna visa att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna dokumenteringsskyldighet. Årsrapporten är även ett medel för personuppgiftsansvarigs uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

2.2 Beskrivning och förklaring av granskningsmetod och resultat

Dataskyddsombudet har granskat verksamhetens dataskyddsarbete utifrån sex obligatoriska områden. De sex områdena har

identifierats genom en analys av kraven i GDPR om hur verksamheter bör arbeta systematiskt med dataskydd. Varje område innehåller ett antal kontrollfrågor som ger en bild av verksamhetens dataskyddsarbete. Dessa områden överensstämmer med de delar som enligt Integritetsskyddsmyndigheten, IMY, utgör grunden för en verksamhets systematiska och rättssäkra hantering av personuppgifter.

I rapporten används en riskmodell med fyra nivåer av risk. Modellen hjälper dataskyddsombudet att visa vilken bedömning hen gör av verksamhetens dataskyddsrisker utifrån de iakttagelser som gjorts i granskningen.

Risknivå	Beskrivning
Hög risk 	Iakttagelsen avser en brist som kan leda till betydande risker för de registrerades rättigheter och friheter. Bristen kräver omgående åtgärd och korrigering.
Medelhög risk 	Iakttagelsen avser en brist som kan leda till risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas skyndsamt, men kräver inte omedelbar korrigering.
Låg risk 	Iakttagelsen avser en brist som kan leda till mindre risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas, men kräver inte omedelbar korrigering.
Inget att anmärka 	Dataskyddsombudet har inga brister att rapportera avseende denna del som kräver åtgärder.

Notera att risken för att tilldelas en sanktion vid tillsyn är större desto högre risken är.

2.3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som personuppgiftsansvarig, PUA, som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som dataskyddsförordningen avser.

De obligatoriska rapporteringsområdena är:

- Registerförteckning
- Tekniska och organisatoriska säkerhetsåtgärder i samband med personuppgifts behandling[1]
- Konsekvensbedömningar
- Överföring till tredje land
- Individens rättigheter
- Personuppgiftsincidenter

Utöver dessa obligatoriska områden rapporteras även om de fördjupade granskningar som skett under föregående år samt planerade granskningsaktiviteter för år 2026. Ett specifikt kapitel om risker och omvärldsbevakning är också prioriterat i rapporten för att underlätta beslut angående dataskyddsarbetet framåt för personuppgiftsansvarig.

[1] I tidigare årsrapporter är denna punkt uppdelat i rubrikerna ”tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar” och ”styrdokument”

3 Resultatsammanställning och centrala iakttagelser inom dataskyddsarbetet

3.1 Registerförteckning

3.1.1 Syftet med området

I GDPR framkommer det att personuppgiftsansvariga (och personuppgiftsbiträden) ska föra ett register över sina personuppgiftsbehandlingar. Registret brukar benämnas ”behandlingsregister” eller ”registerförteckning”. Registret ska finnas tillgängligt i elektronisk form och ska omfatta samtliga personuppgiftsbehandlingar som personuppgiftsansvarig utför. Det ska hållas uppdaterat vilket innebär att det ska uppdateras vid nya eller förändrade personuppgiftsbehandlingar.

Syftet med detta rapporteringsområde är att beskriva om verksamheten har ändamålsenliga rutiner som möjliggör att nya/förändrade personuppgiftsbehandlingar registreras, huruvida personuppgiftsbehandlingar registreras/uppdateras såsom det krävs samt huruvida de uppgifter som är obligatoriska har besvarats kopplat till de registrerade personuppgiftsbehandlingarna.

3.1.2 Resultat

Registerförteckningen har kontrollerats och uppdaterats enligt årshjulet under 2025. Registerförteckningen förs i en Excellfil.

3.1.3 Sammanfattning

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		*16*
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		*Verksamheten arbetar efter årshjul med uppdateringar. Rutinerna finns nedtecknade i styrdokument.*
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska		*JA*

innehålla de behandlingar som personuppgiftsansvarig utför?		
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		*Ja*

3.1.4 DSO ger råd och rekommendationer till PUA

EU-kommissionen ser över dataskyddsförordningen och har bland annat kommit med lättnadsförslag för arbete med registerförteckningen. Personuppgiftsansvarig uppmanas att omvärldsbevaka och implementera eventuella förändringar som behöver göras.

3.2 Tekniska och organisatoriska åtgärder

3.2.1 Syftet med området

Personuppgiftsansvarig ska tillse att personuppgifter skyddas med lämpliga säkerhetsåtgärder, detta för att till exempel undvika att obehöriga får tillgång till uppgifterna, att uppgifterna förloras eller förstörs.

Personuppgiftsansvarig behöver alltid bedöma vilka tekniska- och organisatoriska säkerhetsåtgärder som ska vidtas för de behandlingar som utförs. Till tekniska säkerhetsåtgärder räknas till exempel kryptering, behörighetsbegränsning, pseudonymisering och säkerhetskopiering. Organisatoriska säkerhetsåtgärder avser till exempel interna riktlinjer och rutiner.

För att skapa förutsättningar för att skydda all information inom verksamheten och ha rätt nivå på skyddsåtgärder, ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare.

Genom att använda arbetssättet i metodhandboken värderas informationen utifrån konfidentialitet, riktighet och tillgänglighet. Verktyget KLASSA hjälper sedan till att ta fram tekniska och organisatoriska krav att ställa internt och mot leverantörer. Detta innefattar även bedömning och värdering av personuppgifter. Genom att genomför riskanalyser identifierar informationsägaren risker och väljer åtgärder för att hantera riskerna.

Den personuppgiftsansvariga måste kunna visa hur GDPR efterlevs och att det finns styrdokument och rutiner är en viktig del i detta. Det görs genom att det finns skriftliga, beslutade och kommunicerade styrdokument samt kända rutiner så att medarbetarna vet hur de ska agera avseende frågor som rör dataskydd.

Syftet med detta rapporteringsområde är att redogöra för huruvida DSO bedömer att det tas hänsyn till risker för den registrerade och om dessa beaktas i tillräcklig mån i genomförda informationsklassningar och riskanalyser samt att rätt bedömningen för både tekniska och organisatoriska åtgärder är gjorda. Vidare bedömer DSO också huruvida det finns tillräckligt mycket reglerat om dataskydd i styrdokument och rutiner samt om dessa är tillräckligt implementerade och kända.

3.2.2 Resultat

Varannan månad har ISAM, DSO och dataskyddshandläggare möte. Där har informationsklassningar varit en stående mötespunkt. Utmaningen framöver kommer vara att fånga upp de AI:n som plötsligt implementeras i IT-tjänster och som skapar nya oväntade personuppgiftsbehandlingar. Det saknas AI-riktlinje och strategi inom Stockholm stad vilket gör det svårt för bolaget att agera och ta höjd för egen AI-användning.

3.2.3 Sammanfattning

Fråga/kontroll	Risk	Rekommendationer
Efter ett antal stickprov på genomförda informationsklassningar, bedömer DSO att resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter?		*Verksamheten har rutiner och DSO involveras vid behov.*
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		*Styrande dokument behöver uppdateras med information om AI efter att staden har en AI-riktlinje.*
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		*De styrande dokumenten är kända i organisationen.*

3.2.4 DSO ger råd och rekommendationer till PUA

DSO ger rådet att omvärldsbevaka förändringar som sker i dataskyddsförordningen under 2026 och uppdatera sturande dokument när behov identifieras. Det saknas en AI-riktlinje i staden, när den finns uppmanas STEM att implementera den i sina styrande dokument.

3.3 Konsekvensbedömning avseende dataskydd

3.3.1 Syftet med området

En konsekvensbedömning avseende dataskydd krävs när personuppgiftsansvarig planerar att inleda en personuppgiftsbehandling som innebär hög risk för de registrerade. Huruvida en behandling innebär hög risk eller inte behöver personuppgiftsansvarig avgöra genom att genomföra en s.k. tröskelanalys.

En konsekvensbedömning ska vara genomförd för samtliga behandlingar som innebär hög risk, vilket innebär att personuppgiftsansvarig även behöver kontrollera huruvida denne utför befintliga behandlingar som innebär hög risk. Om högriskbehandlingar utfös för vilka en konsekvensbedömning inte har gjorts, behöver personuppgiftsansvarig genomföra en sådan.

Genom att genomföra en konsekvensbedömning kan personuppgiftsansvarig identifiera risker med en personuppgiftsbehandling, hantera riskerna genom åtgärder och rutiner samt påvisa ansvarsskyldighet. Genom konsekvensbedömningar kan risker identifieras och förebyggas samt korrekta och relevanta skyddsåtgärder identifieras i kravställning på leverantörerna.

Syftet med detta rapporteringsområde är att rapportera huruvida verksamheten har ändamålsenliga rutiner som möjliggör att tröskelanalyser och konsekvensbedömningar genomförs, huruvida sådana genomförs när det krävs samt huruvida personuppgiftsansvarig har genomfört konsekvensbedömningar för de behandlingar som kräver det.

3.3.2 Resultat

Under det gånga året har IMY, Integritetsskyddsmyndigheten levererat mer vägledningar än bestraffningar. Det har bland annat syns genom ett mycket bra material innehållande vägledning och mallar för konsekvensbedömningar. STEM har anpassat sina mallar efter detta.

Ett av de området som fortfarande brister är de stadsgemensamma konsekvensbedömningarna som saknar process. I dagsläget är de

dokument som tas fram alldeles för generellt hållna och har inte haft med verksamhetsrepresentanter eller dataskyddsombud. Det leder till att det blir merarbete lokalt och många frågetecken att försöka reda ut. Det förekommer också händelser där personuppgiftsansvarig tvingas använda en tjänst utan att den är färdigdokumenterad.

3.3.3 Sammanfattning

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		*Det finns ett förklassningsprotokoll där bland annat frågan om personuppgifter lyfts och det ska bifogas en bilaga (ny 2025) som heter tröskelanalys. Bilagan behöver implementeras under 2026.*
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		*En diskussion har tidigare genomförts och dokumentation i handlingsplan och förklassningsprotokoll om frågan om fullständig konsekvensbedömning ska göras. Dokumentationen i det nya protokollet som omnämns ovan behöver implementeras under 2026.*
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		*Lokal nivå- JA*
		Stadsgemensamma konsekvensbedömningar genomförs ad hoc och efter att det är

		nyckelpersoner som tar initiativ. Det behöver bli tydligare process och rollfördelning för att detta ska bli mer effektivt.
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		*Lokal nivå- JA*
		Centrala system delvis
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		*Lokal nivå JA*
		Det finns brister som påtalats av lokala medarbetare till centrala funktioner.

3.3.4 DSO ger råd och rekommendationer till PUA

Det är en kvarstående rekommendation att det tas fram en central process för metod och roller i processen för stadsgemensamma konsekvensbedömningarna, så att de dokumenten kan användas mer effektivt lokalt. Den nya bilagan för tröskelanalys behöver implementeras under 2026.

3.4 Den registrerades rättigheter

3.4.1 Syftet med området

Den registrerade har ett antal rättigheter enligt GDPR. Den registrerade kan bland annat begära tillgång (registerutdrag), rättelse eller radering. Den som är personuppgiftsansvarig har att tillmötesgå en begäran enligt de krav som finns i dataskyddsförordningen. (För registerutdrag säger GDPR 30 dagar och för övriga begäran skyndsamt.)

Syftet med detta rapporteringsområde är att kontrollera huruvida det finns ändamålsenliga mallar samt rutiner för besvarande av rättighetsbegäran, huruvida inkomna begäranden har hanterats inom den tidsram som finns att förhålla sig till samt huruvida svaren till de registrerade, baserat på ett antal stickprov, uppfyller lagkraven.

3.4.2 Resultat

Rutiner finns om begäran inkommer. Då organisationen inte har till huvuduppgift att behandla personuppgifter sker en begäran mycket sällan.

3.4.3 Sammanfattning

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		*Det finns interna instruktioner.*
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		*0*
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?	*N/A*	*Går ej att bedöma då inga utlämnanden skett.*
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?	*N/A*	*Går ej att bedöma då inga utlämnanden skett.*

3.4.4 DSO ger råd och rekommendationer till PUA

Under 2026 kommer kamerabevakning införas i fastighetsbeståndet. Sannolikheten att begäran ökar i inflöde i och med detta. Därför rekommenderas att PUA går igenom sina rutiner och ser till att de är uppdaterade.

3.5 Personuppgiftsincidenter

3.5.1 Syftet med området

Med begreppet personuppgiftsincident avses en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Om en inträffad personuppgiftsincident medför en risk/ konsekvens för fysiska personers rättigheter och friheter ska den anmälas till Integritetsskyddsmyndigheten, IMY, inom 72 timmar från att den upptäckts. Om personuppgiftsincidenten sannolikt leder till hög risk för de registrerade måste individen informeras utan onödigt dröjsmål. Om en personuppgiftsincident inte bedöms vara anmälningspliktig ska den dokumenteras. Det görs i verktyget IA.

Syftet med detta rapporteringsområde är att kontrollera huruvida det säkerställs att samtliga medarbetare har den kunskap som krävs om personuppgiftsincidenter, huruvida det finns ändamålsenliga rutiner för att hantera händelser som kan utgöra personuppgiftsincidenter och huruvida dessa rutiner följs.

3.5.2 Resultat

STEM har inte haft några personuppgiftsincidenter under 2025. Nedan följer en beskrivning av den incident som blev mycket uppmärksammad i media hösten 2025 och som drabbade delar av Stockholm stad. Det finns en hel del lärdomar att dra av den.

Miljödataincidenten

I slutet av augusti 2025 spreds nyheten att IT-tjänsteleverantören Miljödata hade drabbats av en attack. Det tog sedan ett par dagar innan det uppmärksammades för stadsdels- och fackförvaltningarna att även medarbetare där var drabbade. Detta då den centrala HR-avdelningen har påbörjat att implementera deras arbetsmiljöverktyg på delar av staden. Under veckorna som följde och utredningen vidgades klarnade också bilden för alla inblandade. Det som är problematiskt är att främst personuppgiftsansvaret inte var utrett, f.d. anställda och även vissa med skyddad ID har förts över i implementationsfasen. Det förekom även före detta anställda och medarbetare från bolag i några fall av de som läckts. Vid rapportens skrivande har inte slutrapporten förevisats för mig som DSO.

Tydligt är att incidenten kommer leda till en klar syn på vad som behöver göras innan en sådan här personuppgiftsbehandling kan starta och att det gäller även innan man testar tjänster.

3.5.3 Sammanfattning

Fråga/kontroll	Risk	Rekommendationer
Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident?		*Samtliga medarbetare genomgår stadens obligatoriska kurser i dataskydd och informationssäkerhet. Detta sker enligt årshjul.*
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		*Rutiner finns i dataskyddshandboken.*
Hur många personuppgiftsincidenter har dokumenterats under året?		*0*
Hur många personuppgiftsincidenter har anmälts till IMY under året?		*0*

3.5.4 DSO ger råd och rekommendationer till PUA

Som ett led av händelserna med Miljödataincidenten så är det tydligt att det är viktigt att öva och testa sina incidentrutiner. Kommunikationsvägar och förberedelser är A och O då det uppstår mycket snabba behov av beslut och åtgärder. Rådet är att under 2026 öva och testa organisationen med en personuppgiftsincident likt den som drabbade staden 2025. Rollerna i ett incidentteam behöver vara tydliga, kommunicerade och våga även att involvera personer utanför ordinarie kristeam.

3.6 Överföring till tredje land

3.6.1 Syftet med området

För att säkerställa att den nivå av skydd för personuppgifter som ställs i GDPR inte undergrävs, får överföringar av personuppgifter till länder utanför EU/EES (tredje land) endast ske under särskilda förutsättningar. Det innebär att sådan överföring måste stödjas på antingen ett beslut från EU-kommissionen om att landet ifråga upprätthåller en adekvat skyddsnivå, att överföringen omfattas av en lämplig skyddsåtgärd eller i särskilda undantagsfall. Vidare behöver även kompletterade skyddsåtgärder, utöver de lämpliga skyddsåtgärderna, vidtas i vissa fall.

Syftet med detta rapporteringsområde är att rapportera huruvida personuppgiftsansvarig har identifierat de tredjelandsöverföringar som utförs, huruvida personuppgiftsansvarig tillämpar överföringsverktyg på de tredjelandsöverföringar som utförs och om nödvändiga bedömningar har gjorts avseende tredjelandsöverföringarna.

3.6.2 Resultat

När det ska implementeras nya tjänster har diskussionen om tredjelandsöverföringar och risker med dessa lyfts på ett bra sätt. Om en sådan skulle bli aktuell lyfts frågan med DSO och ISAM på ett bra sätt.

3.6.3 Sammanfattning

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		*JA*
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		*Om det skulle förekomma tredjelandsöverföringar dokumenteras det i registerförteckningen och personuppgiftsbiträdesavtalets bilaga.*

Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?	*N/A*	*Har ej varit aktuellt.*

3.6.4 DSO ger råd och rekommendationer till PUA

Sannolikheten att tredjelandsöverföringar kommer öka, är stor i och med att flera IT-leverantörer flyttar sina tjänster från on-prem (egna servrar) till molntjänster. Under 2026 rekommenderas organisationen att arbeta aktivt med att informera utvalda medarbetare om tredjelandsöverföringar. Det finns också ett behov av att bestämma vilken riskaptit verksamheten har för tredjelandsöverföringar exempelvis genom en molnstrategi.

Det är en utmaning att upphandla tjänster och förvirring finns hos leverantörerna om vad som gäller. Därför är det viktigt att verksamheten fortsätter vara en bra kravställare och kan fånga upp otydligheter med rätt frågeställningar till leverantörer

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- *Granskning 1* Granskning Implementation av AI och AI-tjänster

4.2 Syfte

En av dataskyddsombudets viktigaste uppgifter är att övervaka verksamhetens efterlevnad av dataskyddsförordningen. En central del av det arbetet är att göra återkommande granskningar av hur väl dataskyddsförordningen efterlevs. Resultaten av granskningarna påverkar i stor utsträckning vilka beslut verksamheten kan fatta i fråga om dataskyddsåtgärder. För personuppgiftsansvarig är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under det gångna året och vad resultaten av granskningarna är.

Granskningsområdena är planerade och aviserade vid 2023-års dataskyddsrapport.

4.3 Genomförda granskningar och deras resultat

Beskrivning; Granskning 1 Implementation av AI och AI-tjänster

Under år 2024 har flertalet AI-tjänster tillkommit inom IT-världen. Erbjudanden kommer titt som tätt och är av skiftande karaktär och seriositet. Utifrån integritetsperspektivet är det en komplicerad fråga där den registrerades behov av skydd behöver ställas mot en organisationens krav på digitalisering, effektivisering och utveckling.

Syftet är att följa upp hur processen för tjänster som skjuts ut automatiskt från central IT-förvaltning, inte innehåller AI-verktyg som informationsklassificerats och riskbedömts av STEM.

4.4 Resultat

STEM har inte implementerat något AI under 2025. Det saknas dock fortfarande styrande dokument likt en AI-riktlinje för hela staden som sedan STEM kan ta ställning till. Med en strateg för AI kan också STEM bestämma vilka risker organisationen vill ta. Med sådana dokument skulle ett eventuellt införande av en tjänst med AI

bli lättare och tids- och effektivitetsvinster kan dras i verksamhetens arbete.

4.5 DSO ger råd och rekommendationer till PUA

Rådet från DSO är att efterfråga centrala styrdokument likt AI-riktlinje och AI-strategi för att lättare kunna fatta beslut för STEM:s riskaptit vad gäller AI och annan ny teknik. När denna finns behöver den implementeras i STEM:s egna styrande dokument.

5 Risker inom dataskydd

5.1 Sammanfattning

Prioriterade risker inom verksamheten:

- Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (STEM:s) objektförvaltning. (Kvarstår)
- Ny teknik, t.ex. behandling av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation. (Kvarstår)
- Tredjelandsöverföringar (Kvarstår)
- Osäker e-posthantering med personuppgifter (Kvarstår)
- Lagringsytor utan kontroll (Ny)

5.2 Syfte

Verksamheten har ansvar för att göra vissa typer av riskanalyser, så som konsekvensbedömningar och informationsklassningar, men dessa ger inte en heltäckande bild av personuppgiftsriskerna i verksamheten. Dataskyddsombudet behöver som underlag för sin egen planering och sitt löpande arbete ha kontinuerlig överblick över dessa risker, i verksamhetens samtliga personuppgiftsbehandlingar. Exempelvis krävs en sådan överblick för att kunna välja ut vilka områden som bör granskas under det kommande året eller för att avgöra vilka råd som dataskyddsombudet behöver lämna till verksamheten om dataskyddsåtgärder som behöver vidtas.

Under år 2024 har en riskanalys genomförts tillsammans med informationssäkerhetssamordnaren för att hitta gemensamma åtgärder.

Risk beräknas utifrån RISK= Sannolikhet x Konsekvens

Sannolikhet (1 låg - 5 hög):

Låg risk - Inte trolig att inträffa

Hög risk - Kommer med all sannolikhet att inträffa

Konsekvens (1 liten - 5 stor):

Liten konsekvens - Ingen större påverkan

Stor konsekvens - Omfattande, dyrt kan ändra förutsättningarna dramatiskt

Riskvärde

Låg < 4 (riskerna skall bevakas)

Medel 5-14 (riskerna skall hanteras eller elimineras)

Hög > 15 (riskerna skall elimineras)

5.3 Resultatet av riskkartläggningen

5.3.1 Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (STEMS) objektförvaltning

Som tidigare nämnt flera kapitel har det uppstått problem i införande av nya tjänster beroende på resursbrist hos central förvaltning. Detta påverkar implementation av nya gemensamma IT-tjänster och det systematiska arbetet som ska ske löpande i den egna lokala organisationen. En av de anledningar att exempelvis ”Säkra meddelanden” inte införts är då det saknas centralt utsedda ansvarsroller och åtgärder som ska införas inte följs upp eller återrapporteras att de genomförts. Under hösten 2025 har förbättringar skett men som i rapportens framtagande inte har hunnit med att implementeras. Risken fortsätter därmed att bevakas.

	Hög > 15 (riskerna skall elimineras)
X	Medel 5-14 (riskerna skall hanteras eller elimineras)
	Låg < 4 (riskerna skall bevakas)

5.3.2 Ny teknik, t.ex. behandling av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation

Under år 2024 startade efterfrågan på AI och möjligheten att effektivisera arbetet. År 2025 har det blivit än mer vardag och efterfrågan ökar konstant. Då området är nytt och så även lagstiftningen behövs tydlig och transparent dokumentation när en sådan tjänst ska införas. Tyvärr brister ofta dokumentationen från leverantörerna och den som upphandlar verktyget behöver utbilda dem genom kravställning och möten.

Integritetsriskerna är stora då effektiviteten och möjligheten att ta fram ”smarta lösningar” tenderar att gå först i hela samhället. Mitt arbete som dataskyddsombud blir då i dessa införanden än mer viktigt att agera ombud och skydda de registrerades intressen.

En del i denna risk är också att nya funktioner införs i redan befintliga tjänster. Ett exempel på detta är en transkriberingstjänst vid digitala möten. Efter mötet är klart kommer direkt ett AI-genererat protokoll med sammanfattning, beslutspunkter och åtgärder. Det låter bra, men frågorna vi måste ställa oss då är vart sammanställdes informationen? Vem kan ta del av den? Hur känsligt blev materialet i det nya formatet? Osv. AI är ett oerhört bra och kraftfullt hjälpmedel som vi måste använda medvetet och till rätt saker.

AI-förordningen har också tillkommit under 2025 vilket ställer högre krav på den som upphandlar tjänster att ha kontroll på sina informationsflöden.

X	Hög > 15 (riskerna skall elimineras)
	Medel 5-14 (riskerna skall hanteras eller elimineras)
	Låg < 4 (riskerna skall bevakas)

5.3.3 Tredjelandsöverföringar

Det nya inriktningsbeslutet från stadsledningskontoret som kom under hösten 2023 innebar en öppning för bolaget att använda leverantörer som använder sig av tredjelandsöverföringar. Förutsättningen är att verksamheten har en väl utformad exit-plan om överföringsmekanismen ”Data Privacy Framwork” ogiltigförklaras likt ”Privacy Shield” gjorde år 2020 och ”Safe Harbour” innan dess. Flertalet leverantörer har därför börjat luta sig mot andra former av avtal för överföring till tredjeland som resultat av denna osäkra mekanism. Det i sig kräver att leverantörerna är mogna och har förberett sin dokumentation.

Flertalet leverantörer erbjuder idag endast molntjänster och de stora leverantörerna av sådana är amerikanskägda. Därav är detta en risk som behöver uppmärksammas extra.

	Hög > 15 (riskerna skall elimineras)
X	Medel 5-14 (riskerna skall hanteras eller elimineras)
	Låg < 4 (riskerna skall bevakas)

5.3.4 Osäker e-posthantering med personuppgifter

Varje personuppgift som ska hanteras måste behandlas säkert. När en personuppgift e-postas med någon av stadens leveranser sker själva överföringen krypterat, men är okrypterad i in- och utboxen. Det är också inte säkert att maila externt då exempelvis en medborgares adress inte kan kontrolleras på ett tillräckligt bra sätt.

Stadsledningskontoret har tagit fram en tjänst kallad ”Säkra meddelanden” eller ”TDialog”. Kvarstående aktivitet för verksamheten, är att se över och bedöma vad tjänsten kan användas till.

Jag som DSO kan inte rekommendera i dagsläget att tjänsten används efter att jag tagit del av analysmaterialet. Samtidigt är behovet kvarstående från verksamheten att möjligheten att e-posta personuppgifter säkert och krypterat.

Rekommendationen kvarstår att inte använda tjänsten utan att analysmaterialet finns färdigt. Riskerna har inte besvarats av central förvaltning, ny tillsattes november 2025, och informationsmängderna som ska skickas i det är så pass känsligt och skyddsvärt.

X	Hög > 15 (riskerna skall elimineras)
	Medel 5-14 (riskerna skall hanteras eller elimineras)
	Låg < 4 (riskerna skall bevakas)

5.3.5 Lagringsytor utan kontroll

I den nya plattformen Nordic for Zoom (ersätter ZoomX) kommer det finnas möjlighet att dela dokument och skapa egna grupper fritt för samarbete både inom den egna organisationen och med andra. En bra möjlighet, men i en gemensam mapp eller i en samarbetsyta på Sharepoint kan administratörer med särskild behörighet följa upp och gallra information som inte längre är relevant. I Nordic for Zoom finns inte denna administrativa kontroll vilket gör att kraven i dataskyddsförordningen om transparens (registerutdrag) och lagringsminimering inte kan efterlevas.

X	Hög > 15 (riskerna skall elimineras)
	Medel 5-14 (riskerna skall hanteras eller elimineras)
	Låg < 4 (riskerna skall bevakas)

5.4 DSO ger råd och rekommendationer till PUA

- Att ge råd om hur den centrala organisationen ska få mer resurs att utföra sitt arbete är svårt. Men, vi kan belysa utifrån STEM:s perspektiv att det blir svårt att arbeta effektivt när den brister och det tenderar att bygga flaskhalsar.
- Som DSO rekommenderar jag att ni fortsätter vara nyfikna på ny teknik och våga satsa på den. Men, rekommendationen är att göra det med stor medvetenhet och arbeta efter den metod som finns framtagen för informationsklassning, riskanalys och konsekvensbedömning.

- Risken att tredjelandsöverföringsproblematiken kommer att uppstå igen är sannolikt stor. Överföringsmekanismen bygger idag på en demokratisk presidentorder vilken kan

rivas upp av den tillträdande republikanske presidenten under sin mandatperiod 2025–2029. Styrelsen rekommenderas att ta höjd för risken och bestämma aptiten för vad man är villig att riskera när man ingår nya avtal med leverantörer där överföringar till tredjeland sker. Rådet är också att ha en tydlig exitplan och genomlysa marknaden i förstahand inom Sverige och EU/EES.

- Dataskyddsombudet rekommenderar att fortsätta efterfråga dokumentation och åtgärder för att kunna starta tjänsten säkra meddelanden.

- Under arbetet med införande av Nordic for Zoom behöver risken omhändertas. En rekommendation är att minst skapa en organisatorisk åtgärd med rutiner och förbud, om det inte går att tekniskt stänga av filöverföring, begränsa lagringstiden eller på annat sätt kontrollera ytorna.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Då detta är min sista årsrapport lämnar jag detta öppet för efterkommande dataskyddsombud från Serviceförvaltningen att planera.

6.2 Syfte

Som nämnts tidigare är det granskande arbetet en av dataskyddsombudets viktigaste uppgifter. Eftersom dataskyddsombudet ofta har begränsat med tid, behöver granskningsplanen för det nya året utformas med eftertanke. Som en tumregel bör två-tre granskningar ses som en rimlig granskningsinsats under ett verksamhetsår. Granskningsområdena bör lämpligen väljas utifrån ett riskbaserat synsätt, det vill säga att fokus bör ligga på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Därigenom åstadkoms en röd tråd i dataskyddsarbetet från ett verksamhetsår till nästa samtidigt som de största riskerna elimineras eller åtminstone sänks till en mer acceptabel nivå.

7 Omvärldsbevakning

7.1 Tillsynsmyndigheten omorganiseras

Den 1.a januari 2026 omorganiserades Integritetskyddsmyndighetens, IMY:s, operativa del. Det har nu inrättats en avdelning för tillsyn och klagomål och en för vägledning, innovation och teknik. Syftet är att:

- stärka myndighetens förmåga att genomföra riskbaserad tillsyn,
- stärka myndighetens förmåga att ge tydlig och effektiv vägledning samt
- effektivisera myndighetens hantering av klagomål

Sannolikt kommer det här leda till fler tillsyner baserade på klagomål och som pressmeddelandet säger, genomföra riskbaserade granskningar av organisationer. Det innebär att organisationen behöver ha god kontroll över sina dataskyddsrisker och arbeta aktivt med dem.

7.2 Kommande förändringar av Dataskyddsförordningen

Ett förslag har lämnats från Europakommissionen i november på förändringar i dataskyddslagstiftningarna inom EU. Förslaget syftar främst till att öka möjligheten för innovation och minska administrativa krav på mindre verksamheter. Förslaget var helt annorlunda än det som levererades som första utkast sex månader tidigare då fokus var att minska kravet på registerförteckning.

Analysen jag som DSO gör är, att områdets fokusområden svänger fort men tydligt är att en organisation fortsatt behöver vara en tydlig beställare till leverantörer av IT-tjänster och ha kontroll på sina legala- och informationssäkerhetskrav. Behovet av att göra riskanalyser och tänka till före och ta medvetna risker är en viktig fortsatt nyckelaktivitet inom dataskyddsarbetet.

7.3 Tillsyn av Miljödata incidenten

Under hösten 2025 skedde en större personuppgiftsincident hos leverantören Miljödata. Den berörde även delar av Stockholm stad då Stadsledningskontorets HR-avdelning hade beslutat att använda plattformen leverantören erbjöd. Stadsdelsförvaltningarnas medarbetare och tidigare anställda från och med januari 2024 har i och med läckan hamnat på Darknet. (Se vidare under kapitel 3.5.2) Med anledning av IT-angreppet och den efterföljande läckan av personuppgifter har Integritetsskyddsmyndigheten, IMY, beslutat

att inleda granskningar mot Miljödata samt två kommuner och en region som har använt företagets tjänster. (Göteborgs stad, Älmhults kommun och Region Västmanland)

Urvalet av de granskade aktörerna har gjorts baserat på typ av verksamhet som bedrivs och indikationer på risker då det var många aktörer berörda. Det finns i nuläget inga planer på ytterligare granskningar från IMY men det är heller inte uteslutet att det kommer att ske. Granskningarna kommer bli vägledande i hur en organisation måste agera innan en personuppgiftsbehandling sker.

7.4 Övrigt

IMY har mer fokus på vägledning än bestraffning sedan ett år tillbaka. Det innebär att en organisation kan söka delaktighet i regulatoriska sandlådor där man testar sig fram till ex. ett nytt AI skulle kunna användas.

Under år 2025 lättades kamerabevakningslagen upp. Ett område som troligen kommer att granskas under 2026 av tillsynsmyndigheten är nog att efterlevnaden av lagen, dokumentationskrav och bedömningar.