Stockholms stad

Bilaga 03
GDPR årsrapport

År 2025

GDPR årsrapport
Januari 2026

Dnr: SÖD 2025/984
Utgivningsdatum: 2026-02-19
Kontaktperson: Anna Remmets

Sammanfattning

GDPR, eller dataskyddsförordningen, syftar till att skydda individers grundläggande rättigheter och friheter, med särskilt fokus på rätten till skydd av personuppgifter. I Stockholms stad är varje nämnd och styrelse ansvarig för personuppgiftsbehandlingar som sker i den egna verksamheten. Ett dataskyddsombud (DSO) har i uppdrag att oberoende granska verksamhetens efterlevnad av dataskyddsförordningen. I denna rapport redovisar DSO årets granskning av Södermalms stadsdelsnämnds dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

Sammantaget fortsätter arbetet med dataskydd på förvaltningen att utvecklas och förbättras. Detta till stor del därför att man har satsat på att utveckla informationssäkerhetsarbetet som helhet. Det är viktigt att detta arbete kan fortsätta utvecklas. Den centrala samordningen med normerande klassningar och referenskonsekvensbedömningar har också förbättrats, men det finns fortfarande stora utmaningar i hur detta organiseras, hur dokumentation delas och när i projekten lokala informationssäkerhetssamordnares (ISAM:s) och DSO:er bjuds in.

Dokumentationen av personuppgiftsbehandlingar på förvaltningen i systemet DraftIt är centralt i dataskyddsarbetet men fortsätter att vara en utmaning. Arbetssätt och resurser behöver därför ses över under 2026.

I övrigt händer mycket med ny teknik, säkerhetsläget i omvärlden, och nationell lagstiftning som kan påverka informationssäkerhet och integritetsskydd (se granskningarna och stycket Omvärldsbevakning i bilaga) som behöver följas.

Förvaltningen har inga allvarliga risker (bedöms röda) vilket är positivt. Att bara något enstaka granskningsområde är utan brister (bedöms grönt) beror på att det innebär att i princip inga ytterligare åtgärder krävs, vilket är svårt att uppnå.

De tre största riskerna enligt dataskyddsombudets bedömning

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
1.Registreras/uppdateras behandlingar [i personuppgiftsförteckningen] i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför? *2. Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning*		Se över arbetssätt med personuppgiftsförteckningen och dataskyddsredogörarnas resurser.

avseende dataskydd görs samt genomfört detta?		
3. (Från övrig granskning Inbyggt dataskydd och dataskydd som standard) *Tas dataskydd i beaktande vid upphandling av nya tjänster och utveckling av nya arbetssätt?*		De system med riskfyllda personuppgiftsbehandlingar som ännu inte har informationsklassats behöver identifieras och informationsklassas och konsekvensbedömningar genomföras.
		Staden centralt behöver fortsätta utveckla arbetet med normerande informationsklassningar, t.ex. när det gäller att ha kompletta klassningsprotokoll, tillgängliga åtgärdsplaner och en samordnad internkontroll i staden för att så sker samt att samordnat informera ut till förvaltningar och bolag när nya normerande klassningar är klara så att förvaltningarna som i många fall är personuppgiftsansvariga men använder centralt upphandlade system har den information som krävs för att kunna genomföra lokala klassningar av hög kvalitet men på ett mer effektivt och ändamålsenligt sätt.

Innehållsförteckning

Inledning

Dataskyddsförordningen (GDPR), syftar till att skydda individers grundläggande rättigheter och friheter, med särskilt fokus på rätten till skydd av personuppgifter. GDPR sätter tydliga ramar för hur personuppgifter får behandlas för att minimera risken för skada och säkerställa att hanteringen sker ansvarsfullt och rättvist. GDPR har sin grund i de mänskliga rättigheterna, där varje individ har rätt till respekt för sitt privat- och familjeliv samt skydd av sina personuppgifter.

I Stockholms stad är varje nämnd och styrelse ansvarig för personuppgiftsbehandlingar som sker i den egna verksamheten.

Dataskyddsombudets uppgift

Varje personuppgiftsansvarig (nämnd eller styrelse) ska utse ett dataskyddsombud (DSO). DSO:s uppgifter framgår direkt av lagstiftningen. Ombudets roll är att kontrollera att GDPR följs inom organisationen. Det innebär bland annat att ge råd, rekommendationer och informera om frågor som rör behandlingar av personuppgifter. DSO har även i uppdrag att oberoende granska verksamheternas arbete med dataskyddsfrågor för att säkerställa att GDPR efterlevs. DSO ska rapportera direkt till högsta förvaltnings-/bolagsnivå. I Stockholms stad innebär det att DSO rapporterar till nämnder och styrelser.

DSO lämnar årligen en rapport om verksamhetens dataskyddsarbete till varje nämnd och styrelse. Genom rapporten kan nämnd och styrelse ta emot råd och rekommendationer. Årsrapporten syftar till att nämnd/styrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Årsrapporten är ett medel för nämndens/styrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Granskning av dataskyddsarbetet 2025

Kontroll av obligatoriska områden

DSO 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.

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

Resultatsammanställning och centrala iakttagelser inom dataskyddsarbetet

I detta avsnitt presenteras en sammanställning av den bedömda risknivån för verksamhetens dataskyddsarbete, grundat på kontrollfrågorna inom de sex obligatoriska områdena. Vidare redovisas DSO:s centrala iakttagelser, inklusive områden där verksamheten uppvisar goda resultat och bör upprätthålla sitt arbete, samt identifierade brister som kan utgöra dataskyddsrisker. Avsnittet innehåller även rekommenderade åtgärder för att hantera dessa risker och stärka dataskyddsarbetet.

En fullständig redovisning av DSO:s underlag och resultat från granskningen av de sex obligatoriska områdena finns att läsa i bilaga 1. Bilagan innehåller även en beskrivning av syftet och bakgrunden för varje område.

Register över personuppgiftsbehandlingar

Sammanfattning

För att personuppgifterna ska kunna skyddas måste de vara kända för verksamheten. Det följer därför i klartext av GDPR (artikel 30) att stadens alla förvaltningar och bolag måste inventera alla personuppgifter som behandlas i verksamheten, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde, och dokumentera dem i en så kallad registerförteckning (även kallat behandlingsregister).

På Södermalms stadsdelsförvaltning är det särskilt sociala avdelningen, avdelningarna för förskola och äldreomsorg och stab och kansli som har registrerat många personuppgiftsbehandlingar i verktyget DraftIt som används för ändamålet. Detta är positivt eftersom det är inom socialtjänst, äldreomsorg och förskola som den största mängd känsliga personuppgifter avseende personer i beroendeställning behandlas.

Övriga avdelningar bör se över vilka verksamhetsprocesser som behöver läggas in.

Samtliga avdelningar bör även se över hur processerna/personuppgiftsbehandlingarna är avgränsade och formulerade. Önskvärt är att de avspeglar stadens klassificeringsstruktur.

Vad gäller uppdateringarna har förvaltningens dataskyddsredogörare haft svårt att få in svar och rutinen för detta kommer behöva ses över under 2026.

Det finns dock bättre förutsättningar nu än tidigare att fånga upp nya personuppgiftsbehandlingar då förvaltningen har intensifierat och bättre samordnar sitt informationssäkerhetsarbete.

Bedömning av risknivå och rekommendationer från DSO

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		Alla avdelningar, i synnerhet de som i nuläget har registrerat relativt få personuppgiftsbehandlingar behöver se till att samtliga verksamhetsprocesser där personuppgifter behandlas dokumenteras.
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		Rutiner finns men behöver bli mer kända och eventuellt revideras om det fortsätter att finnas utmaningar med att dokumentera personuppgiftsbehandlingar och säkerställa att förteckningen är uppdaterad.
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		Se sammanfattningen ovan. Svar på uppdateringsfrågorna har i vissa fall inte inkommit eller varit bristfälliga.
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		Till stor del, men kvaliteten på svaren varierar. De säkerhetsåtgärder som ska dokumenteras behöver ofta stämmas av mot informationsklassning och där behövs ett ökat samarbete mellan dataskyddsredogörare och lokala objektledare i verksamheterna.

Säkerhet i samband med behandlingen

Sammanfattning

För att personuppgifter ska få rätt skydd är det viktigt att dataskydd beaktas redan när nya arbetssätt införs eller tekniska lösningar tas i bruk. Dataskydd är därför en central del i de informationsklassningar som enligt stadens riktlinje för informationssäkerhet ska genomföras vid upphandling/införskaffning av nya system.

Även om det är nämnden som är personuppgiftsansvarig och chefer, såsom framgår av tillämpningsanvisning och lokal anvisning för informationssäkerhet, har ett stort ansvar för arbetet med dataskydd är också alla medarbetare skyldiga att i sitt dagliga arbete efterleva de regler som finns. Därför behöver rutiner och styrdokument som är uppdaterade och lättillgängliga finnas på plats och dessa behöver vara kända. Styrdokument och rutiner behövs också för att kunna leva upp till GDPR:s krav på ansvarsskyldighet, det vill säga visa hur förvaltningen arbetar för att leva upp till lagens krav.

Arbetet med informationsklassningar på förvaltningen har under de senaste två åren intensifierats och rutinen har förbättrats. Då informationssäkerhetssamordnare (ISAM) och DSO har ett nära samarbete i och med informationsklassningarna har dataskyddet beaktats. Det är därför av betydelse att informationssäkerhet även framöver får resurser för att kunna upprätthålla detta arbete.

Vad gäller de normerande klassningarna är det mycket positivt att staden arbetar med dessa men det finns fortfarande utmaningar med att samla rätt kompetens och få in dataskydd i rätt del av projektet så att DSO:s rekommendationer verkligen kan hörsammas innan beslut fattas. Vid bristande normerande klassningar riskerar förvaltningar och bolags lokala bedömningar skilja sig åt vilket blir ett hinder för likställighet i staden och skapar risk för frustration i verksamheterna när olika förvaltningar gör olika bedömningar.

ISAM och DSO kommer under 2026 att fortsätta utveckla rutiner för att kontrollera att de åtgärder som beslutas vid informationsklassningar genomförs. För att skapa en struktur för detta behöver förvaltningen fortsätta att implementera PM3.

Styrdokument och rutiner bör bli mer kända, förslagsvis genom att de även fortsättningsvis tas upp i lokal utbildning i informationssäkerhet och dataskydd och kommuniceras på arbetsplatsträffar (APT) och i nyhetsbrev.

Bedömning av risknivå och rekommendationer från DSO

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?		Förvaltningens DSO medverkar i eller ser över de informationsklassningar som görs så inga stickprov har behövts. De lokala informationsklassningarna tar hänsyn till de kategorier av personuppgifter som förekommer i objekten, men det har funnits utmaningar med de normerande informationsklassningarna (se sammanfattning).
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		Det finns både centrala och lokala dokument och dessa är uppdaterade. Det är viktigt att de fortsätter uppdateras och att det finns ett tydligt ägarskap.
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		Styrdokument och rutiner skulle behöva bli mer kända. Förslagsvis genom att de även fortsättningsvis tas upp i lokal utbildning i informationssäkerhet och dataskydd och kommuniceras på APT och i nyhetsbrev.

Konsekvensbedömning avseende dataskydd

Sammanfattning

Om en personuppgiftsbehandling leder till hög risk för de registrerades integritet och rättigheter, till exempel om en stor mängd uppgifter behandlas, om känsliga uppgifter och/eller personuppgifter om personer i beroendeställning, samt om ny teknik används, kan en så kallad konsekvensbedömning behöva göras. I en sådan tittar man närmare på riskerna för specifikt integritet och beskriver vilka åtgärder som vidtas för att skydda personuppgifter.

Det finns mall och rutin för hur och när konsekvensbedömningar ska genomföras och förvaltningen arbetar aktivt med informationsklassningar där behov av konsekvensbedömning identifieras. För att upprätthålla goda förutsättningar för att identifiera behov och genomföra konsekvensbedömningar bör förvaltningen fortsätta att implementera PM3 och säkerställa att resurser för informationssäkerhetsarbete finns.

[redacted]

ISAM och DSO kommer under 2026 se över rutinen för uppföljning av åtgärder som beslutats i informationsklassning och konsekvensbedömningar.

Bedömning av risknivå och rekommendationer från DSO

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		Staden har inte haft någon mall för tröskelanalys, men under 2025 har Integritetsskyddsmyndigheten (IMY) tagit fram en som kan användas. Tröskelanalys har ändå i praktiken gjorts i samband med informationsklassningar.
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		Se svaret ovan.
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		Det finns en central mall samt lokala och centrala rutiner.
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		Behov av konsekvensbedömning identifieras vid informationsklassning. [redacted]

		[redacted]
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		Se svaret ovan.

Den registrerades rättigheter

Sammanfattning

Enligt bestämmelserna i GDPR har de registrerade rätt att bland annat få information om behandling av deras uppgifter och även invända mot behandlingen och begära rättelse, radering och begränsning. Dessa rättigheter är dock inte absoluta då ändring och radering hos myndigheter styrs av annan lagstiftning. En begäran måste handläggas även om den avslås och den registrerade ska enligt GDPR få svar senast efter en månad (i undantagsfall kan detta förlängas).

Av de begäranden som kommit till DSO:s kännedom under 2025 har enbart en besvarats efter längre tid än en månad. Detta berodde på komplexiteten i begäran.

DSO fortsätter under 2026 att ge stöd i att besvara inkomna förfrågningar och granskar om det kommit in några under 2025 som inte kommit till DSO:s kännedom.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		DSO fortsätter att bevaka området och ser över behov av uppdateringar i rutin och mall.
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		Åtta begäranden har kommit till DSO:s kännedom. DSO har skickat ut granskningsfrågor om antalet inkomna begäranden via förvaltningens dataskyddsredogörare men i skrivande stund januari 2026 inte fått svar.
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		Sju av de åtta som DSO har kännedom om.
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		Verksamheterna bör även fortsatt vid behov ta stöd av DSO för att formulera svaren och DSO följer upp utvecklingen på området genom till exempel domar.

Personuppgiftsincidenter

Sammanfattning

Antalet rapporterade personuppgiftsincidenter har ökat i jämförelse med 2024 (se nedan). Detta beror delvis på att Serviceförvaltningen, som är personuppgiftsbiträde åt stadsdelsförvaltningarna har börjat rapportera in fler incidenter. En större benägenhet att rapportera incidenter, både på förvaltningen och hos biträden, är positivt, men det finns ända anledning att under 2026 hålla koll på om ökningen beror på någon brist i rutiner eller liknande. De vanligaste incidenterna består i att uppgifter skickats fel, vilket oftast beror på den mänskliga faktorn. Alla verksamheter bör dock se över sina rutiner för mejl- och postutskick etc. så att risken för fel kan minska.

Det förekommer fortfarande att personuppgiftsincidenter inte rapporteras som sådana till DSO, utan upptäcks vid DSO:s månadsvisa kontroll i IA, men i mindre utsträckning nu än tidigare. Detta visar att rutinen för incidenthantering behöver bli mer känd på förvaltningen. Detta kan ske på utbildningar, i nyhetsbrev och på APT.

En incident som stack ut under 2025 var den som skedde hos leverantören Miljödata. Stadsdelsförvaltningarna har inte kunnat ta del av utredningen i någon större omfattning, men händelsen väcker frågor om den centrala informationsklassningen av systemet Stella och vilka bedömningar som gjordes innan man lade in den stora mängden uppgifter i en testmiljö. Incidenten visar också på vikten av att staden centralt utvecklar arbetet med normerande klassningar så att förvaltningarna i sin tur kan uppfylla sina åtaganden som personuppgiftsansvariga.

Bedömning av risknivå och rekommendationer från DSO

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?	🟡	Lokal rutin finns på intranätet och medarbetare och chefer påminns om denna på utbildningar och i nyhetsbrev. Cheferna ska även informera på APT, men detta har inte varit dokumenterat i de stickprov som genomförts. En reflektion är att vid nästa granskning göra mer omfattande stickprovskontroll.
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?	🟡	Se ovan. Till stor del följs de, men det förekommer fortfarande händelser i avvikelsehanteringssystemet IA som är personuppgiftsincidenter men som inte rapporterats som sådana.
Hur många personuppgiftsincidenter har dokumenterats under året?	🟡	31 stycken. (23 stycken 2024). Ökningen beror till stor del på att serviceförvaltningen som är personuppgiftsbiträde för förvaltningen har infört en ny rutin för att

		rapportera in incidenter, vilket är positivt liksom att benägenheten att rapportera incidenter är hög. Dock bör rutiner där det är möjligt ses över så att incidenter i högre grad undviks.
Hur många personuppgiftsincidenter har anmälts till IMY under året?		Tolv stycken. (Sex stycken 2024). Av de incidenter som bedömts som så allvarliga att de behövt rapporteras till IMY har merparten inträffat i förvaltningens hantering och inte biträdenas. Siffran är inte alarmerande och rapporteringsbenägenheten är positiv men det finns anledning för verksamheterna att se över rutiner för att i högre grad undvika incidenter.

Överföring till tredje land

Sammanfattning

Överföring av personuppgifter till tredje land kan uppstå när en leverantör har servrar och/eller ägare i ett land utanför EU/EES. Även om inga uppgifter aktivt förs över kan det tredje landet ha lagstiftning som till exempel gör att leverantören kan bli skyldig att lämna ut uppgifter till landets myndigheter. GDPR reglerar när en tredjelandsöverföring är tillåten, till exempel när standardavtalsklausuler används eller det tredje landet omfattas av ett adekvansbeslut. Inför överföring till tredje land kan det vara nödvändigt att genomföra en särskild riskanalys, en så kallad Transfer Impact Assessment (TIA).

Det absolut vanligaste landet som är aktuellt i sammanhanget är USA. USA omfattas i nuläget av ett adekvansbeslut förutsatt att leverantören ifråga är ansluten till EU-U.S Data Privacy Framework. Den politiska utvecklingen i USA gör dock att framtiden för detta adekvansbeslut är osäker, och verksamheterna behöver därför vara restriktiva i användningen av tjänster som innebär överföring till USA (och andra tredje länder) samt ha en exitplan på plats.

Det är också viktigt att fortsatt arbeta strukturerat med informationsklassningar så att eventuella tredjelandsöverföringar kan identifieras.

Bedömning av risknivå och rekommendationer från DSO

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		Genomförandet av informationsklassningar säkerställer att tredjelandsöverföringar identifieras. Förvaltningen behöver dock fortsätta arbetet med att klassa samtliga av sina informationstillgångar och verksamheterna behöver säkerställa att det finns rutiner för användning av olika tjänster så att överföring till tredje land om möjligt undviks.
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		De överföringar som är identifierade omfattas av adekvansbeslutet för de amerikanska företag som är del av EU-U.S. Data Privacy Framework. Detta adekvansbeslut kan dock komma att omprövas i en nära framtid.
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		Avseende de överföringar som är identifierade har TIA gjorts när det bedömts som nödvändigt. TIA behöver egentligen inte genomföras när överföringen omfattas av adekvansbeslut, men enligt stadens inriktningsbeslut för tredjelandsöverföringar bör någon typ av riskanalys ändå göras.

Bilagor

Bilaga 1: Detaljerad redovisning av dataskyddsombudets granskning

Bilaga 2: Andra genomförda granskningar och omvärldsbevakning

Bilaga 1 - Detaljerad redovisning av dataskyddsombudets granskning

Denna bilaga innehåller en beskrivning av syftet med respektive obligatoriskt område samt en mer detaljerad redovisning av dataskyddsombudets (DSO:S) granskning och slutsatser. Här framgår vilka iakttagelser som gjorts och vilken information som samlats in under granskningsarbetet av de sex obligatoriska rapporteringsområdena. För varje område redovisas de underlag som har använts, de iakttagelser som har gjorts samt hur dessa har utgjort grunden för dataskyddsombudets riskbedömning och rekommenderade åtgärder.

1. Register över personuppgiftsbehandlingar

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 rapportera 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.

Kontroller och iakttagelser gjord av dataskyddsombudet

Förvaltningens DSO granskar under året hur många behandlingar som är inlagda i verktyget DraftIt. DSO skickar även via dataskyddsredogörarna ut uppdateringsfrågor till samtliga avdelningar för att säkerställa att förteckningen är korrekt och uppdaterad. För övriga iakttagelser, se stycket Register över personuppgiftsbehandlingar i rapporten.

Antal behandlingar som är registrerade?

348.

Har verksamheten ändamålsenliga rutiner som möjliggör att nya/förändrade behandlingar registreras?

Förvaltningens dataskyddsredogörare skickar regelbundet ut kontrollfrågor till avdelningarna för att säkerställa att personuppgiftsförteckningen är uppdaterad och korrekt. I samband med att informationsklassningar genomförs ställs frågan om personuppgiftsbehandlingen är registrerad.

Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?

Det har varit utmaningar med att få in svar på uppdateringsfrågorna och svaren tyder vissa gånger på att frågorna och syftet med inte helt förståtts. DSO ska tillsammans med ISAM

under 2026 utveckla rutinen för att följa upp de åtgärder som tas fram vid informationsklassningar, varav registrering av personuppgiftsbehandlingar är en.

Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?

Till stor del, men kvaliteten på svaren varierar. De säkerhetsåtgärder som ska dokumenteras behöver ofta stämmas av mot informationsklassning och där behövs ett ökat samarbete mellan dataskyddsredogörare och lokala objektledare.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Enligt årsrapport för 2024 var de registrerade behandlingarna då flera. DSO avser att utreda vad detta beror på, men ett möjligt svar är att samma behandlingar tidigare registrerats dubbelt av olika avdelningar. Färre registreringar innebär inte per automatik ett sämre resultat, utan kan tvärtom vara ett tecken på minskning av dubbelregistreringar och att verksamheterna närmare följer stadens klassificeringsstruktur för processer. Hur verksamhetsprocesser formuleras och avgränsas i DraftIt är något som DSO tillsammans med förvaltningens dataskyddsredogörare behöver fortsätta att titta på under 2026.

I övrigt inga markanta skillnader från föregående år.

Dataskyddsombudets bedömning samt rekommendationer

Se kapitel Register över personuppgiftsbehandlingar i rapporten.

2. Säkerhet i samband med behandlingen

Bakgrund och syfte

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

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

För att skapa förutsättningar för att skydda information (inklusive personuppgifter) med rätt slags skydd 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 riskanalyser identifierar informationsägaren risker och väljer åtgärder för att minska riskerna. Risker i samband med

personuppgiftsbehandling är en typ av risk som informationsägaren behöver omhänderta i riskanalyser.

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

Syftet med detta rapporteringsområde är därmed att rapportera huruvida DSO bedömer att det tas hänsyn till risker för den registrerade och om dessa beaktas i tillräcklig mån i genomförda informationsklassningar och riskanalyser. Vidare bedömer DSO huruvida det finns tillräckligt mycket reglerat om dataskydd i styrdokument och rutiner samt om dessa är tillräckligt implementerade och kända.

Kontroller och iakttagelser gjord av dataskyddsombudet

DSO har medverkat under de informationsklassningar som genomförts på förvaltningen och har då kunnat säkerställa att dataskyddet tagits i beaktande. DSO har även granskat lokala och centrala styrdokument. Verksamheterna ombeds rapportera i ILS vilka styrdokument som är kända för medarbetarna och hur dessa har gjorts kända.

För övriga iakttagelser, se kapitlet Säkerhet i samband med behandlingen.

Dataskyddsombudets jämförelse med föregående års resultat

Inga betydande förändringar.

Dataskyddsombudets bedömning samt rekommendationer

Se kapitel Säkerhet i samband med behandlingen i årsrapporten.

3. Konsekvensbedömning avseende dataskydd

Bakgrund och syfte

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 utförs 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.

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.

Kontroller och iakttagelser gjord av dataskyddsombudet

DSO har kontrollerat vilka konsekvensbedömningar som är genomförda och jämfört mot dokumentation från informationsklassningar och personuppgiftsförteckningen.

För övriga observationer, se kapitel Konsekvensbedömning avseende dataskydd i årsrapporten.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Inga stora skillnader. Användandet av ny teknik såsom AI, inte minst inom välfärden har dock inneburit ett visst ökat behov av att genomföra konsekvensbedömningar. Det centrala arbetet har också till viss del utvecklats och lokala DSO:er bjuds in till referenskonsekvensbedömningar i högre grad än tidigare.

Dataskyddsombudets bedömning samt rekommendationer

Se kapitel Konsekvensbedömning avseende dataskydd i årsrapporten.

4. Den registrerades rättigheter

Bakgrund och syfte

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.

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.

Kontroller och iakttagelser gjord av dataskyddsombudet

DSO har gått igenom inkomna begäranden som kommit till DSO:s kännedom samt skickat ut frågor till avdelningarna via dataskyddsredogörarna om dessa få begäranden som inte gått via DSO. I skrivande stund har inte frågan besvarats men kommer att följas upp under 2026. För övriga iakttagelser, se kapitel Den registrerades rättigheter i årsrapporten.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Ingen betydande förändring.

Dataskyddsombudets bedömning samt rekommendationer

Se kapitel Den registrerades rättigheter i årsrapporten.

5. Personuppgiftsincidenter

Bakgrund och syfte

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 för fysiska personers rättigheter och friheter ska den anmälas till IMY inom 72 timmar från upptäckt. Om personuppgiftsincidenten sannolikt leder till hög risk för de registrerade måste de informeras utan onödigt dröjsmål.

Om en personuppgiftsincident inte bedöms vara anmälningspliktig ska den dokumenteras.

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.

Kontroller och iakttagelser gjord av dataskyddsombudet

Förvaltningens DSO för logg över de incidenter som rapporteras samt kontroller varje månad incidentrapporteringsverktyget IA för att upptäcka incidenter som inte har rapporterats som personuppgiftsincidenter.

För övriga iakttagelser, se kapitel Personuppgiftsincidenter i årsrapporten.

Dataskyddsombudets jämförelse med föregående års resultat

Se kapitel Personuppgiftsincidenter i årsrapporten.

Dataskyddsombudets bedömning samt rekommendationer

Se kapitel Personuppgiftsincidenter i årsrapporten.

6. Överföring till tredje land

Bakgrund och syfte

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.[1]

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.

Kontroller och iakttagelser gjord av dataskyddsombudet

DSO har tillgång till dokumentation från informationsklassningar, konsekvensbedömningar och personuppgiftsförteckning där förekomsten av tredjelandsöverföring ska anges.

För övriga iakttagelser, se kapitel Överföring till tredje land i årsrapporten.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Förutsättningarna för att identifiera tredjelandsöverföringar har blivit bättre i och med ett strukturerat informationssäkerhetsarbete. Förändringar av den politiska situationen i USA gör att adekvansbeslutets fortsatta giltighet är ännu mer osäkert än tidigare.

Dataskyddsombudets bedömning samt rekommendationer

Se kapitel Överföring till tredje land i årsrapporten.

[1] Europeiska dataskyddsstyrelsens (EDPB) Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överenstämmelsen med EU-nivån för skydd av personuppgifter, Version 2.0, Antagna den 18 juni 2021.

Bilaga 2 – Andra genomförda granskningar och omvärldsbevakning

Andra granskningar som dataskyddsombudet har genomfört under året

Genomförda granskningar och deras resultat

Granskning 1: Autentisering (SÖD 2025/549)

Autentisering är en viktig del av skyddet av personuppgifter. För system som behandlar känslig information krävs ofta flerfaktorsautentisering, det vill säga en kombination av till exempel lösenord, tjänstekort eller andra autentiseringsmekanismer.

Merparten av informationsklassningarna som genomförts på förvaltningen avseende verksamhetssystem som behandlar känsliga personuppgifter anger att flerfaktorsautentisering används. Vad gäller olika delar av sociala system, där en stor del av de känsligaste personuppgifterna finns, saknas dock svar i dokumentation från informationsklassningar.

Detta kan bero på att underlagen kommer från normerande klassningar som tidigare har saknat många svar.

Granskning 2: Inbyggt dataskydd och dataskydd som standard (SÖD 2025/549)

För att kunna säkerställa ett skydd för personuppgifter som lever upp till GDPR:s krav behöver den personuppgiftsansvariga redan vid anskaffningen av tjänster/system och påbörjandet av nya arbetssätt se till att rutiner och tekniska lösningar motsvarar lagstiftningens krav på integritetsskydd.

Detta kallas inbyggt dataskydd och dataskydd som standard.

I nästan samtlig av den dokumentation som granskats finns exempel på rutiner och tekniska lösningar som främjar integritet.

Några exempel är flerfaktorsautentisering med bl. a. SITHS-kort och BankID, begränsad lagringstid och rekommenderade förinställningar som minimerar personuppgiftsbehandling.

Det intensifierade arbetet på förvaltningen med informationsklassningar ökar möjligheten att kontrollera förekomsten av inbyggt dataskydd och dataskydd som standard på en detaljerad nivå. Ett problem i sammanhanget har dock varit tekniska frågor i vissa fall har varit svåra att få besvarade från leverantörerna.

Införandet av verktyget Tempus i förskolan, där den centrala styrgruppen beslutade om en lösning för skyddade personuppgifter som flera av stadens DSO:er invände mot visar på fortsatta utmaningar och vikten av att fortsätta utveckla arbetet med normerande klassningar i staden.

Det finns risker med ny teknik med många olika funktioner varav en del bygger på AI, som i den digitala trygghetstjänst för äldreomsorgen som planeras införas.

Det är viktigt att rutiner kring skyddade personuppgifter finns och följs.

Dataskyddsombudets rekommendationer (baserade på iakttagelserna ovan)

1. Förvaltningen bör fortsätta att kommunicera till staden centralt att kompletta normerande klassningar där de tekniska frågorna utreds är viktiga för att förvaltningarna ska kunna bedöma sin lokala förmåga att skydda de personuppgifter man hanterar.
2. Förvaltningen behöver i anskaffande av nya system etc. beakta informationssäkerhet tidigt.
3. Arbetet med informationsklassningar och uppföljning av dessa bör fortsätta.
4. Förvaltningen bör fortsätta arbeta med att utse lokala objektledare och säkerställa att a-klassningar (informationsklassning innan upphandling/driftsättande) genomförs.
5. Fortsatt kommunikation med staden centralt om vikten av arbete med normerande klassningar och att tillräckligt mycket tid avsätts.
6. Genom informationsklassningar säkerställs att tekniska svar av god kvalitet från leverantören inkommer.
7. DSO bör kopplas in tidigt i processen inför upphandling av nya system eller införande av ny personuppgiftshantering både lokalt och centralt
8. Riskfyllda behandlingar prioriteras vid klassningar

Omvärldsbevakning

Tekniken inom AI fortsätter att utvecklas vilket innebär både möjligheter och utmaningar som kommer att ställa krav på dataskyddsarbetet på förvaltningen. Samtidigt är en stor del av den teknik som används av svenska myndigheter helt eller delvis amerikansk. Den politiska utvecklingen i USA kommer säkerligen påverka hur svenska kommuner förhåller sig till detta och vilka åtgärder som kommer krävas.

I november 2025 publicerade EU-kommissionen ett åtgärdspaket som innebär relativt stora förändringar i tolkningen av dataskyddsförordningens bestämmelser. Det handlar till exempel om när uppgifter ska betraktas som knutna till en individ, kraven på konsekvensbedömningar och registrerades rättigheter. Förändringarna är tänkte att förenkla ett regelverk som upplevs som krångligt. Detta kan vara positivt för verksamheter som upplever lagstiftningen som snårig och resurskrävande, men kan också komma att inverka negativt på skyddet av enskildas integritet.

Nationellt ser vi dessutom olika lagförslag som innebär större möjlighet att dela sekretesskänsliga uppgifter mellan myndigheter, kamerabevaka och i högre utsträckning genomföra bakgrundskontroller vid rekrytering. Allt detta försvagar integritetsskyddet i helhet och det är därför viktigt att verksamheterna också tar GDPR:s bestämmelser i beaktande vid tillämpning av dessa lagar.

Övrigt att rapportera

Inget övrigt att rapportera.