Stockholms stad

Bilaga 3

GDPR årsrapport

År 2025

Äldrenämnden

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 har i uppdrag att oberoende granska verksamhetens efterlevnad av dataskyddsförordningen. I denna rapport redovisar dataskyddsombudet årets granskning av förvaltningsnämndens dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

I egenskap av Dataskyddsombud (DSO) lämnar vi följande årsrapport.

De tre största riskerna enligt dataskyddsombudets bedömning:

GDPR årsrapport 2025
December 2025

Dnr: ALD 2026/5
Utgivningsdatum: 2026-01-07
Kontaktpersoner: Nils-Erik Lundborg, Peter Sundström

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
Hanteringen och uppföljningen av PUB-avtal		Samtliga huvudavtal där Äldreförvaltningen står som ansvarig för upphandlingen av systemet eller tjänsten bör granskas för att säkerställa att där det behövs finns ett korrekt och undertecknat PUB-avtal. Utöver det bör äldreförvaltningen inhämta kunskap om vad som gäller för övriga tjänster eller system som förvaltningen använder och som exempelvis upphandlats centralt.
Registerförteckning och genomföra konsekvensbedömningar/Minimering av incidenter		Utreda rutiner och arbetssätt som minskar/minimerar risken att personuppgifter hanteras felaktigt, exempelvis genom att de sprids till obehöriga/fel mottagare.
Fortsatt genomförande av pågående dataskyddsarbete		Under 2025 har det genomförts ett omfattande arbete för att skapa styrdokument och rutiner för hanteringen av personuppgifter i enlighet med GDPR. Det kvarstår vissa delar innan arbetet kan övergå i förvaltning. Det arbetet måste slutföras. Även efter det bör det finnas tillräckliga resurser för kompetensutveckling och möjlighet att bibehålla det genomförda arbetet.

Innehållsförteckning

Inledning

GDPR, eller dataskyddsförordningen, syftar till att skydda individers grundläggande rättigheter och friheter, med särskilt fokus på rätten till skydd av personuppgifter. Dataskyddsreglerna (*kallas GDPR fortsättningsvis*) 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. Dataskyddsombudets 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. Dataskyddsombudet har även i uppdrag att oberoende granska verksamheternas arbete med dataskyddsfrågor för att säkerställa att dataskyddslagstiftningen efterlevs. DSO ska rapportera direkt till högsta förvaltnings-/bolagsnivå. I Stockholms stad innebär det att dataskyddsombudet rapporterar till nämnder och styrelser.

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

Granskning av dataskyddsarbetet

Kontroll av obligatoriska områden

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.

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

Resultat från granskningen av de sex obligatoriska områdena

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

En fullständig redovisning av dataskyddsombudets 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

Under våren 2025 har det tagits fram en ny registerförteckning som innefattar alla de uppgifter som krävs enligt art. 30 GDPR. Förteckningen är upprättad i Excelformat och hålls tillgänglig för förvaltningen i den gemensamma mappen Aldre_Gemensam.

I samband med granskningen av förvaltningens behandlingar visade det sig att förvaltningen efter upphandlingen av privata hemtjänstleverantörer och dagverksamhet enligt huvudavtalet blir personuppgiftsbiträde i förhållande till leverantörerna. Det följer av huvudavtalet, Hemtjänst - Stockholms stad, att leverantörerna ska behandla vissa uppgifter i rapporteringssystem inom Paraplyet. Enligt art 30 p 2 ska personuppgiftsbiträden föra ett register över de behandlingar som utförs för den personuppgiftsansvariga. En sådan förteckning har upprättats som också hålls tillgänglig för förvaltningen i den gemensamma mappen Aldre_Gemensam.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		57 personuppgiftsbehandlingar har registrerats i Äldrenämndens registerförteckning. Förteckningen påbörjades under vintern 2024/2025 och är nu uppdaterad med flertalet av nämndens personuppgiftsbehandlingar. Arbete pågår med kartläggning av personuppgiftsbehandlingar inom området personaladministration och digital utveckling.
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		En rutin för återkommande översyn av registret har införts. Rutinen innebär att äldreförvaltningens dataskyddshandläggare i början av året går igenom och reviderar

		registret med hjälp av kontaktpersoner inom verksamheterna.
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		Registret och rutinerna har etablerats under 2025 och hanteringen behöver därför följas upp under kommande år.
Innehåller registret de uppgifter som är obligatoriska enligt artikel 30 (namn och kontaktuppgifter på den personuppgiftsansvarige, ändamål, kategorier av registrerade, mottagare, eventuell tredjelandsöverföring, gallringstider (om möjligt) samt en kort beskrivning av säkerhetsåtgärderna)?		Den framtagna registerförteckningen omfattar samtliga punkter i artikel 30. Vidare finns uppgift om och när det har gjorts en konsekvensbedömning.

Säkerhet i samband med behandlingen

Sammanfattning

Arbetet med informationsklassningen är eftersatt och ISAM har startat ett arbete med informationsklassning av förvaltningens system och information. Det innebär att det varit svårt att granska klassningarna.

Vår iakttagelse är att det i staden finns en genomarbetad mall för informationsklassning och i den finns ett avsnitt med dataskyddsfrågor. Samtidigt finns det mallar för risk- och konsekvensbedömningar av personuppgiftsbehandlingar. Dessa görs separat och det är oklart hur de bör hänga ihop. Det kan vara något att arbete vidare på inom äldreförvaltningen.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

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?		Såvitt är känt tas tillräcklig hänsyn till de olika kategorierna av personuppgifter i samband med informationsklassningar.
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		Ja.
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		Ja, såvitt är känt.

Konsekvensbedömning avseende dataskydd

Sammanfattning

Vid årets början hade det endast gjorts en konsekvensbedömning, personuppgiftsbehandlingar i tjänsten Nyckelfri hemtjänst. Konsekvensbedömningen genomfördes 2022, i samband med upphandlingen av tjänsten. När tjänsten nu är i drift bör bedömningen ses över och revideras.

Under våren har behandlingarna som utförs inom avdelningen Stockholms trygghetsjour granskats och tre konsekvensbedömningar genomförts. Bedömningarna omfattar de behandlingar som utförs i samband med:

1. Besvara inkomna larm via larmmottagningen och biståndsbedömning m.m. (utförs inom enheterna Larmmottagning och Jourenheten,
2. Köhantering för vård- och omsorgsboende, servicehus och förmedling av platser till korttidsboende, och
3. Installation och service av trygghetslarm.

Föreslagna säkerhetsåtgärder bör följas upp. Det finns också anledning att granska vissa behandlingar närmare i samband med att utvecklingsinsatser genomförs.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		Under 2025 har det utarbetats rutiner för genomförandet av konsekvensbedömningar i äldreförvaltningen. Staden har också reviderat de generella mallarna och instruktionerna för konsekvensbedömningar vilka har använts för de senaste bedömningarna.
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		Ja.
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		I den framtagna mallen för analys av personuppgiftsbehandlingar finns ett avsnitt som beskriver kriterierna och hur tröskelanalysen ska genomföras. Dataskyddshandläggaren ansvarar för att analysen görs.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		Ja, såvitt är känt.
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		Det har genomförts konsekvensbedömningar av de personuppgiftsbehandlingar som utförs inom kärnverksamheterna. Dessa bör revideras i samband med att föreslagna säkerhetsåtgärder vidtagits. Konsekvensbedömningar rörande klagomål, avvikelsehantering, Lex Sarah-utredningar och personaladministration är under genomförande.

Den registrerades rättigheter

Sammanfattning

Mallar och rutiner för hantering av registrerades rättigheter har tagits fram och publicerats.

Under våren 2025 har informationen till registrerade uppdaterats på stadens hemsida stockholm.se och på Intranätet.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	**Risk**	**Rekommendationer**
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		Ja, sedan 2025.
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		Hittills har det inkommit en (1) begäran om registerutdrag.
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		Samtliga.
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		Ja, enligt uppgift från tidigare dataskyddsombud som hade uppdraget fram till och med september 2025.

Personuppgiftsincidenter

Sammanfattning

Incidenthanteringen inom förvaltningen har uppmärksammats i samband med att förvaltningens personuppgiftsbehandlingar har analyserats. Det som kan noteras är att fler incidenter rapporteras i jämförelse med förra året. Det kan förklaras med att det efter information och diskussioner i samband med granskningen av personuppgiftsbehandlingar uppmärksammats att det är viktigt att alla incidenter utreds och därför bör rapporteras.

Den absolut vanligaste incidenten är att e-postmeddelanden om insatser skickas till fel mottagare. Efter granskningarna av de berörda behandlingarna beslutades att det skulle vidtas säkerhetsåtgärder med syfte att minimera risken för återkommande incidenter. Här är förvaltningens ISAM och chefen för Jourenheten drivande arbetet.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

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?		Information på Intranätet med mallar för hur incidenterna ska hanteras. Årlig intern utbildning och återkommande samtal i samband med APT-möten.
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		Det finns rutiner. Det kan emellertid ifrågasättas om dessa är tillräckligt ändamålsenliga givet det låga antalet inrapporterade incidenter.
Hur många personuppgiftsincidenter har dokumenterats under året?		Hittills 17 inkl. Miljödata-incidenten. Antalet incidenter har ökat sedan förra årets redovisning. Ökningen kan främst förklaras med att fler incidenter anmäls via IA och därför blir kända.
Hur många personuppgiftsincidenter har anmälts till IMY under året?		En (1) incident [Miljödata-incidenten].

Överföring till tredje land

Sammanfattning

Flertalet verksamhetssystem som innebär någon form av personuppgiftsbehandling som äldreförvaltningen använder är system som tillhandahålls centralt. Utgångspunkten har därför varit att eventuell överföring till tredje land har gjorts i samband att systemen upphandlats och införts.

För det system som äldreförvaltningen upphandlat för trygghetslarmet, UMO, har det inte gjorts en TIA. Vid granskningen av systemet och i samband med uppgraderingen av systemet uppdagades att det bifogade Personuppgiftsbiträdesavtalet var en mall. Den saknade uppgifter om leverantörer och underleverantörer och var inte underskrivet. Det har därför påbörjats ett samtal med leverantörens svenska kontakt för att utreda vilka som är underleverantörer och var de finns placerade geografiskt. Frågan behöver prioriteras.

Frågan kompliceras av att leverantören Enovation Ltd har sitt säte i Storbritannien men att det framkommit uppgifter om att ett franskt företag har tagit över ägandet av Enovation och den aktuella verksamheten. Detta är emellertid inte något av avgörande betydelse för bedömningen eftersom Frankrike är ett EU-land och, som sådant, omfattas av dataskyddsförordningen och det skyddsramverk som finns däri.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		Delvis.
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		Frågan behöver utredas såtillvida att det inte är klarlagt exakt i vilka behandlingar tredjelandsöverföringar sker. Denna brist har lyfts och är av hög prioritet. I den mån eventuell tredjelandsöverföring sker kan verksamheten sannolikt stödja sig på gällande adekvansbeslut för överföringar av personuppgifter mellan EU/EES och USA.
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		Nej. Detta kan utgöra en potentiell risk om det, mot förmodan, skulle visa sig att verksamheten använder behandlingssystem som innebär att personuppgifter överförs till tredjeland som inte omfattas av ett adekvansbeslut.

Bilagor

Bilaga 1: Detaljerad redovisning av dataskyddsombudets granskning

Bilaga 2: Rekommendationer 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 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

Antal behandlingar som är registrerade?

57 behandlingar.

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

Ja, rutiner finns. Det är emellertid vår bedömning att dessa rutiner behöver kommuniceras och förankras ute i verksamheten för att säkerställa att dessa rutiner efterlevs.

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

Delvis. Det återstår visst arbete med att kontrollera vilka behandlingar som eventuellt innebär överföring av personuppgifter till tredjeland.

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

Ja.

Dataskyddsombudets jämförelse med föregående års resultat

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

Ett omfattande arbete har lagts ned på att se över registerförteckningen och att säkerställa att förvaltningen har relevanta PUB-avtal med leverantörerna.

Dataskyddsombudets bedömning samt rekommendationer

Verksamheten har det senaste året lagt betydande resurser på att se över och komplettera sin registerförteckning. Det återstår nu att närmare kontrollera att eventuella högriskbehandlingar konsekvensbedöms samt att det finns tydlig dokumentation gällande användningen av molntjänster och tredjelandsöverföring. Detta arbete bör prioriteras.

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

Efter ett antal stickprov på genomförda informationsklassningar, bedömer DSO att resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter?

Ja, såvitt är känt.

Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?

Ja, såvitt kan bedömas finns det tillräckligt mycket stöd och rutiner för att verksamheten ska kunna uppfylla kraven på informationssäkerhet och integritet.

Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?

Ja, såvitt är känt.

Dataskyddsombudets jämförelse med föregående års resultat

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

Verksamheten lägger numera ett större fokus på dessa frågor.

Dataskyddsombudets bedömning samt rekommendationer

Uppfattningen är att detta inte har varit tillräckligt högt prioriterat tidigare, men att det nu sker en positiv förändring, inte minst tack vare det faktum att förvaltningen tagit hjälp av ett externt dataskyddsombud under 2025 som har lyft dessa frågor på agendan. Detta arbete behöver emellertid fortsätta och bedömningen är att det finns ett stort behov av ökad kunskap ute i verksamheterna utöver behovet av mer ändamålsenliga rutiner och arbetssätt.

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 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.

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

Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?

Ja.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

Ja.

Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?

Ja.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

Ja, såvitt är känt.

Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?

Ja, såvitt är känt.

Dataskyddsombudets jämförelse med föregående års resultat

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

Vi ser en positiv tendens då verksamheten har lagt mera fokus på dessa frågor under det senaste året.

Dataskyddsombudets bedömning samt rekommendationer

Även om verksamheten har rutiner för genomförandet av konsekvensbedömningar saknar förvaltningen en tydlig metodik för att tidigt fånga upp och bedöma risker kopplat till behandlingen av olika kategorier av personuppgifter. Redan i samband med informationsklassningen bör dessa frågor lyftas och i viss mån bedömas och inte endast i samband med konsekvensbedömningen i ett senare skede.

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

Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?

Ja.

Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?

En (1) begäran om registerutdrag.

Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?

Samtliga [en begäran].

Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?

Ja, såvitt är känt.

Dataskyddsombudets jämförelse med föregående års resultat

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

Situationen är ungefär den samma som föregående år.

Dataskyddsombudets bedömning samt rekommendationer

Den sammanlagda bedömningen är att verksamheten har rutiner och arbetssätt för att kunna hantera inkommande begäranden i enlighet med dataskyddsförordningen.

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 Integritetsskyddsmyndigheten (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

Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident?

Genom att regelbundet informera de anställda om vikten av att rapportera misstänkta personuppgiftsincidenter samt rutinerna för detta.

Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?

Ja, det är dock dataskyddsombudets uppfattning att det finns ett betydande mörkertal när det kommer till det faktiska antalet incidenter i förhållande till vad som faktiskt rapporteras i IA.

Hur många personuppgiftsincidenter har dokumenterats under året?

17 incidenter.

Hur många personuppgiftsincidenter har anmälts till IMY under året?

En (1) incident [Miljödata-incidenten].

Dataskyddsombudets jämförelse med föregående års resultat

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

Situationen är ungefär den samma som föregående år.

Dataskyddsombudets bedömning samt rekommendationer

Bedömningen är att verksamheten bör fokusera mer på att informera de anställda om vanligt förekommande typer av incidenter (exempelvis på APT-möten) och vikten av att dokumentera dessa så att verksamheten kan dra lärdom och därigenom utveckla arbetssätt och processer.

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

[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.

Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?

Delvis. Frågan behöver utredas såtillvida att det inte är klarlagt exakt i vilka behandlingar tredjelandsöverföringar sker. Denna brist har lyfts och är av hög prioritet.

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?

I den mån eventuell tredjelandsöverföring sker kan verksamheten sannolikt stödja sig på gällande adekvansbeslut för överföringar av personuppgifter mellan EU/EES och USA.

Har nödvändig bedömning, ”Transfer Impact Assessment” (TIA), gjorts avseende tredjelandsöverföringarna?

Nej. Detta kan utgöra en potentiell risk om det, mot förmodan, skulle visa sig att verksamheten använder behandlingssystem som innebär att personuppgifter överförs till tredjeland som inte omfattas av ett adekvansbeslut.

Dataskyddsombudets jämförelse med föregående års resultat

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

Ingen skillnad jämfört med föregående år.

Dataskyddsombudets bedömning samt rekommendationer

Eftersom det i verksamheten saknas fullständig information om vilka behandlingar som eventuellt innebär överföring av personuppgifter till tredjeland behöver verksamheten prioritera arbetet med att identifiera dessa behandlingar eftersom det dels kan innebär en otillåten risk (om det rör sig om känsliga uppgifter), dels en potentiell risk i det fall EU-kommissionens adekvansbeslut skulle ogiltigförklaras.

Bilaga 2 – Rekommendationer och omvärldsbevakning

Dataskyddsombudets rekommendationer baserat på iakttagelserna ovan

Dataskyddsombudets rekommendationer
1. *Ett mer genomgripande arbete återstår med att utreda verksamhetens olika personuppgiftsbehandlingar och eventuella tredjelandsöverföringar,* 2. *Verksamheten behöver se över rutinerna för hanteringen av personuppgiftsincidenter. Det kan ifrågasättas om dessa är tillräckligt ändamålsenliga givet det låga antalet inrapporterade incidenter.* 3. *Verksamheten bör säkerställa att det finns tillräckliga resurser för att kunna arbeta systematiskt med dataskyddsfrågor.*

Omvärldsbevakning

Resultatet av dataskyddsombudets omvärldsbevakning

EU-kommissionens adekvansbeslut gällande tredjelandsöverföringar av personuppgifter mellan EU/EES och USA överprövades efter att en fransk parlamentariker påtalat vad han ansåg var fundamentala brister i skyddet för de registrerade och som inte i tillräcklig utsträckning hade beaktats vid beslutet. EU-domstolen meddelade dock sommaren 2025 att beslutet skulle stå fast. I och med detta har kommunen kunnat fortsätta med vissa behandlingar som innebär överföring av personuppgifter till USA.