Stockholms stad

Bilaga 4

GDPR årsrapport

År 2025

Idrottsnämnden

GDPR årsrapport 2025
December 2025

Dnr: IDF 1.1.2/2026/10
Utgivningsdatum: 2026-01-08
Kontaktpersoner: Nils-Erik Lundborg, Peter Sundström

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:

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
Registerförteckning – behov av översyn och komplettering		Kontroll och revidering för år 2025 pågår. Detta är ett arbete som behöver prioriteras.
Incidenthantering – behov av att se över rutiner och utbildning i samtliga led inom verksamheten		Verksamheten bör se över sina rutiner och arbetssätt för att öka medvetenheten om vikten av att rapportera incidenter så att verksamheten kan arbeta proaktivt och minimera riskerna kopplat till verksamhetens personuppgiftshantering. Antalet rapporterade personuppgiftsincidenter är orealistiskt lågt.
Verksamhetens arbete med rutiner och styrdokument		Det återstår att arbete inom verksamheten med att se över och uppdatera befintliga styrdokument kopplat till riskbedömningar, konsekvensbedömningar och kravställningar i personuppgiftsbiträdesavtal. Även detta arbete bör prioriteras. Verksamheten bör lägga mer resurser på kompetensutveckling och kvalitetssäkring i dataskyddsarbetet.

Innehållsförteckning

Sammanfattning 1
Inledning 3
Dataskyddsombudets uppgift 3
Granskning av dataskyddsarbetet 4
Kontroll av obligatoriska områden 4
Resultat från granskningen av de sex obligatoriska områdena 5
Register över personuppgiftsbehandlingar 5
Säkerhet i samband med behandlingen 7
Konsekvensbedömning avseende dataskydd 8
Den registrerades rättigheter 9
Personuppgiftsincidenter 10
Överföring till tredje land 11
Bilagor 12
Bilaga 1 - Detaljerad redovisning av dataskyddsombudets granskning ... 13
Bilaga 2 – Rekommendationer och omvärldsbevakning 21

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

Registerförteckningen ska uppdateras/kontrolleras under hösten och vintern 2025 parallellt med ett pågående arbete kring verksamhetens arkivhantering. Därutöver pågår ett arbete med att skapa nya hanteringsanvisningar tillsammans med en konsult från Stadsarkivet.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		93 personuppgiftsbehandlingar har registrerats i Idrottsnämndens registerförteckning. Det saknas åtminstone två behandlingar i förteckningen.
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		Delvis. Det finns ett behov av att se över rutinerna för att säkerställa att verksamheten på ett bättre sätt kan upprätthålla en komplett och uppdaterad förteckning. Detta arbete bör prioriteras då vissa behandlingar i sin tur kan föranleda ett krav på att genomföra en konsekvensbedömning i syfte att hantera eventuella risker för de registrerade.
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		Nej, men det pågår ett arbete med att se över och komplettera registret.

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)?		Delvis. Detta gäller såvitt är känt för de behandlingar som finns registrerade i registerförteckningen. Förteckningen är dock inte helt komplett. Men ett arbete pågår med att komplettera den.

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 idrottsförvaltningen.

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?		Kontroller och revidering har inte slutförts i sin helhet såvitt avser registrerade behandling.
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		Delvis, men det finns ett behov av att se över rutiner och att kommunicera och förankra dessa på ett tydligare sätt i verksamheten.
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		Nej.

Konsekvensbedömning avseende dataskydd

Sammanfattning

Konsekvensbedömning har genomförts för processerna kring bokningsförfarandet samt i samband med pågående uppdatering av it-stödet för föreningsstöd och schemaläggning i samma program.

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

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		Delvis. Det finns emellertid tecken på att detta sker mer sporadiskt snarare än metodiskt och rutinmässigt. Staden har reviderat de generella mallarna och instruktionerna för konsekvensbedömningar vilka har använts för de senaste bedömningarna.
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		Delvis. Jämför med kommentaren ovan.
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		Det finns tecken som visar på ett dessa rutiner inte är tillräckligt ändamålsenliga och förankrade i verksamheten.
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 följas upp och i vissa fall revideras.

Den registrerades rättigheter

Sammanfattning

Det finns mallar för hantering av registrerades rättigheter. Dessa hanteras av registraturen.

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, såvitt är känt.
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		Inga begäranden har inkommit detta år.
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		Eftersom verksamheten inte har fått några begäranden har således inga besvarats.
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		Det finns rutiner för detta. Frågan kvarstår huruvida dessa rutiner i praktiken skulle följas i händelse av en begäran om exempelvis registerutdrag.

Personuppgiftsincidenter

Sammanfattning

Det har under året endast rapporterats två incidenter varav en har rapporterats till IMY. Det låga antalet rapporterade incidenter internt kan endast förklaras av att det finns en okunskap kring vad en personuppgiftsincident och/eller kring betydelsen av att rapportera misstänkta personuppgiftsincidenter i syfte att belysa dessa internt som en betydande risk, inte enbart för de registrerade utan även för verksamheten i sin roll som en samhällsviktig aktör i kommunen.

Det som kan noteras att antalet incidenter är på samma låga nivå som tidigare.

Den absolut vanligaste incidenten är att e-postmeddelanden skickas till fel mottagare. Efter samtal med verksamhetens informationssäkerhetssamordnare (ISAM) har vi kommit fram till att det behöver vidtas åtgärder för att lyfta betydelsen av att rapportera misstänkta incidenter i syfte att minimera risken för återkommande incidenter. Här är förvaltningens ISAM drivande i det 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?		Det finns viss information för hur incidenter ska hanteras. Det orealistiskt låga antalet rapporterade incidenter talar dock för att det behövs en informations- eller utbildningsinsats i verksamheten.
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		Det finns enligt verksamheten ändamålsenliga rutiner. Det är emellertid tveksamt att dessa följs givet det orealistiskt låga antalet rapporterade incidenter.
Hur många personuppgiftsincidenter har dokumenterats under året?		Hittills en (1) [Miljödata-incidenter]. Antalet incidenter ligger på samma låga nivå som föregående år.
Hur många personuppgiftsincidenter har anmälts till IMY under året?		En [Miljödata-incidenten].

Överföring till tredje land

Sammanfattning

Flertalet verksamhetssystem som innebär någon form av personuppgiftsbehandling som idrottsförvaltningen 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.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		Svårt att avgöra. Det saknas behandlingar i registerförteckningen. Verksamheten arbetar dock med att komplettera och uppdatera förteckningen.
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		Verksamheten stödjer sig på EU-kommissionens adekvansbeslut för överföringar av personuppgifter mellan EU/EES och USA (EU-US DPF).
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		Nej, verksamhetens tredjelandsöverföringar sker i enlighet med förutsättningarna givna i EU-US DPF.

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?

93 behandlingar.

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

Det finns rutiner, men det ifrågasättas huruvida dessa är ändamålsenliga givet det faktum att det saknas behandlingar i registerförteckningen.

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

Nej.

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

Delvis. Såvitt är känt gäller detta endast för de behandlingar som finns registrerade i förteckningen. Förteckningen är inte komplett.

Dataskyddsombudets jämförelse med föregående års resultat

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

Nej, resultatet är att jämställa med föregående år.

Dataskyddsombudets bedömning samt rekommendationer

Hela registerförteckningen ska enligt verksamheten uppdateras/kontrolleras under hösten och vintern 2025 parallellt med ett pågående arbete kring arkivhantering och nya hanteringsanvisningar som genomförs tillsammans med en konsult från stadsarkivet. Vidare är en pågående genomlysning av HR-området pågående.

Bedömningen är att verksamheten är väl medveten om de brister som finns när det kommer till registerförteckningen och behovet av ändamålsenliga rutiner men att åtgärder nu vidtas för att komma tillrätta med dessa bister. Detta arbete sker i nära samarbete med förvaltningens informationssäkerhetssamordnare.

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 kan bedömas.

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

Delvis. Det saknas ändamålsenliga rutiner för att säkerställa att verksamheten konsekvent och metodiskt analyserar tänkta behandlingar utifrån dataskyddsregelverkets krav på säkerhet för olika kategorier av personuppgifter.

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

Nej. Det återstår ett arbete för verksamheten att på ett tydligare sätt än hittills kommunicera dessa och förankra rutiner och styrande dokument i verksamheten.

Dataskyddsombudets jämförelse med föregående års resultat

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

Nej, situationen skiljer sig inte åt nämnvärt från föregående år.

Dataskyddsombudets bedömning samt rekommendationer

Med anledning av att det i verksamheten delvis saknas ändamålsenliga rutiner för ett riskbaserat informationssäkerhetsarbete, bör detta arbete prioriteras. Eventuella risker behöver fångas upp i ett tidigt skede, delvis med utgångspunkt i den informationsklassning som ska ske i samband med nya behandlingar och processer.

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, delvis.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

Ja, såvitt är känt.

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

Ja, verksamheten använder sig av stadens mall för konsekvensbedömningar.

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?

Nej, situationen är ungefär den samma som föregående år.

Dataskyddsombudets bedömning samt rekommendationer

Verksamheten har rutiner för genomförandet av konsekvensbedömningar. Desto mer osäkert är verksamhetens rutiner för att systematiskt och metodiskt fånga upp eventuella risker i tidigt skede av nya behandlingar och processer genom exempelvis s.k. tröskelanalyser. Dessa kan med fördel göras parallellt med att informationsklassningen görs.

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?

Inga begäranden har inkommit detta år.

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

Eftersom verksamheten inte har mottagit någon har heller ingen begäran besvarats.

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

Omöjligt att svara på men rutiner finns för att kunna hantera en begäran i enlighet med dataskyddsförordningen.

Dataskyddsombudets jämförelse med föregående års resultat

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

Nej, situationen kan jämföras med föregående år.

Dataskyddsombudets bedömning samt rekommendationer

En allmän reflektion (som inte är unik för denna förvaltning) är att det finns ett behov av en ökad medvetenhet i verksamheterna kring vilka rättigheter de registrerade har och hur man ska hantera en rättighetsbegäran. Det faktum att inte en enda begäran har registrerats centralt i förvaltningen kan sannolikt vara ett tecken på att det finns en okunskap kring dels hur dessa begäranden ska besvaras men framförallt att dessa ska dokumenteras och registreras centralt i förvaltningen. Rekommendationen är att verksamheten undersöker detta och vidtar eventuella åtgärder.

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?

Det finns rutiner, men verksamheten behöver lägga resurser på att utbilda och regelbundet informera de anställda om typiska personuppgiftsincidenter. Detta kan förslagsvis ske på APT-möten eller liknande möten.

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

Det finns rutiner för detta. Verksamheten behöver dock lägga ytterligare resurser på att kommunicera dessa rutiner i samtliga verksamhetsgrenar för att i större utsträckning uppmärksamma misstänkta personuppgiftsincidenter. Det orealistiskt låga antalet rapporterade incidenter är ett tydligt tecken på detta behov.

Hur många personuppgiftsincidenter har dokumenterats under året?

En (1) [Miljödata-incidenten].

Hur många personuppgiftsincidenter har anmälts till IMY under året?

En (1) [Miljödata-incidenten].

Dataskyddsombudets jämförelse med föregående års resultat

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

Nej, resultatet skiljer sig inte nämnvärt åt från föregående år.

Dataskyddsombudets bedömning samt rekommendationer

Verksamheten har uppmärksammat behovet av att informera om vikten av att rapportera misstänkta personuppgiftsincidenter. Detta arbete är en viktig del i de anställdas förståelse för behovet av tydliga rutiner och ett systematiskt och konsekvent arbetssätt.

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

Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?

Svårt att avgöra. Det återstår visst arbete med att komplettera registerförteckningen.

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?

Det rättsliga stödet för verksamhetens tredjelandsöverföringar grundar sig på EU-kommissionens adekvansbeslut för överföringar av personuppgifter mellan EU/EES och USA (EU-US DPF).

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

Nej, se svar ovan.

Dataskyddsombudets jämförelse med föregående års resultat

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

Nej.

Dataskyddsombudets bedömning samt rekommendationer

Rekommendationen är att verksamheten dels ser över samtliga behandlingar i registerförteckningen, dels de behandlingar som ännu inte finns registrerade för att identifiera eventuella tredjelandsöverföringar.

[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 – Rekommendationer och omvärldsbevakning

Dataskyddsombudets rekommendationer baserat på iakttagelserna ovan

Dataskyddsombudets rekommendationer
1. *Verksamheten bör satsa mer resurser på dataskyddsfrågorna för att bättre kunna hantera löpande såväl som akuta frågor.* 2. *Arbetet med registerförteckningen behöver prioriteras.* 3. *Verksamheten behöver systematisera arbetet med tröskelanalyser och konsekvensbedömningar.*

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.