Stockholms stad

Bilaga 9

GDPR årsrapport

År 2025

Kulturnämnden

GDPR årsrapport 2025
December 2025

Dnr: KUN 2025/32
Utgivningsdatum: 2026-02-17
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 två största riskerna enligt dataskyddsombudets bedömning:

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
Kontroll och Uppföljningen av PUB-avtal		Kulturförvaltningen är personuppgiftsansvarig för en rad olika system och med detta följer ett ansvar för att säkerställa att där det behövs finns ett korrekt och undertecknat PUB-avtal. Förvaltningen uppger att man inte har följt upp tidigare ingångna PUB-avtal och att det i vissa fall har gått många år sedan dessa avtal upprättades. Rekommendationen är därför kulturförvaltningen kontrollerar/följer upp leverantörernas hantering av personuppgifter och eventuella förändringar i underbiträdenas personuppgiftshantering.
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

Kulturförvaltningen arbetar med att uppdatera och komplettera registerförteckningen, och detta arbete kommer att fortsätta under hösten och vintern 2025. I förteckningen anges om det rör sig om tredjelandsöverföring, exempelvis Sociala medier. Mer tveksamt om det finns angivet gällande Microsoft 365.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		44 personuppgiftsbehandlingar har registrerats i Kulturnämndens registerförteckning. Förteckningen bedöms i allt väsentligt vara komplett, men visst arbete återstår med att kontrollera de leverantörer och eventuella underbiträden som utför behandlingen på uppdrag av verksamheten för att identifiera eventuella förändringar som kan ha inverkan på laglighet, säkerhet och lämplighet.
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		Ja. Registret uppdateras i samband med att nya behandlingar sker samt i samband med upphandling av nya system och tjänster som innebär en ny personuppgiftsbehandling.

Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		Ja, såvitt är känt.
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)?		Registerförteckningen är huvudsakligen komplett, men det återstår visst arbete med att se över de behandlingar som sker hos leverantörer och underbiträden för att säkerställa att förvaltningen har aktuella uppgifter av betydelse för verksamhetens efterlevnad av GDPR art. 30.

Säkerhet i samband med behandlingen

Sammanfattning

Arbetet med tröskelanalyser och konsekvensbedömningar är eftersatt och behöver ses över. Det pågår emellertid ett arbete med att konsekvensbedöma behandlingarna i tre olika system och processer, närmare bestämt kamerabevakning, Kollo och Biblioteksystem. Därutöver bör verksamheten genomföra en konsekvensbedömning avseende Speedadmin där känsliga personuppgifter kan förekomma. Ett helhetsgrepp behöver tas för att säkerställa att verksamheten har analyserat och hanterat alla potentiella högriskbehandlingar.

Följande riskmitigerande åtgärder har emellertid genomförts under 2025 inom processen för kulturskolans elevadministration (som primärt stöds av SpeedAdmin):

- Utbildning i gällande rutiner och användning av systemet, tex att undvika exporter, maila från systemet och att vara försiktig med fritextfält,
- Extra uppföljning med rapportering till enhetschefer av vilka medarbetare som genomgått de årliga dataskydds- och informationssäkerhetskurserna,
- Security awareness training med fejkat nätfiske,
- Pågående leverantörsdialog om gallringsfunktionen, backuprutiner och loggar

Planerade åtgärder för 2026:

- Upprätta systemplan med kontinuitetsplanering,
- Rutin för granskning av åtkomsträttigheter,
- Framtagande av nya gallringsbeslut.

Dataskyddsombudens 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. Utmaningen tycks ligga i att på ett tydligt sätt kommunicera och förankra dessa rutiner och mallar i de olika verksamheterna där personuppgiftsbehandlingarna de facto sker.

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?		Ja, såvitt är känt.

Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		Ja, såvitt är känt.
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		Delvis. Det återstår för verksamheten att på ett tydligare sätt kommunicera relevanta rutiner och styrdokument så att dessa förankras på samtliga nivåer inom verksamheten, exempelvis rutiner för behörighetsstyrning.

Konsekvensbedömning avseende dataskydd

Sammanfattning

I skrivande stund har en konsekvensbedömning genomförts för det nya biblioteksystemet. Det pågår ett arbete med att bedöma behandlingarna i tre olika system och processer, närmare bestämt biblioteksystemet, kamerabevakning och Söka kollo. Därutöver bör verksamheten genomföra en konsekvensbedömning avseende Speedadmin där känsliga personuppgifter kan förekomma. Ett helhetsgrepp behöver således tas för att säkerställa att verksamheten har analyserat och hanterat alla potentiella högriskbehandlingar.

Föreslagna åtgärder bör följas upp och kontrolleras under kommande år. Det finns också anledning att granska vissa behandlingar närmare i samband med att leverantörerna genomför tekniska förändringar och/eller anlitar nya underbiträden.

I övrigt kan nämnas att med utgångspunkt i de av Serviceförvaltningen upprättade rutinerna för tröskelanalys och konsekvensbedömning har verksamheten tagit fram en liten guide, och om den godkänns kan den publiceras på förvaltningens intranät.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		Ja, såvitt är känt.
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		Ja, tröskelanalyser genomförs vid nya/förändrade behandlingar. Dessutom genomförs en årlig översyn. Positivt är att tröskelanalyser genomförs parallellt med informationsklassning och eventuella it-säkerhetsfrågor för att fånga upp eventuella risker redan i det skedet.
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		Ja. Verksamheten använder Integritetsskyddsmyndighetens mall för konsekvensbedömning.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		Det finns brister när det kommer till att genomföra och upprätta konsekvensbedömningar. Verksamheten har identifierat fem behandlingar som kräver att konsekvensbedömning genomförs. Två av dessa har genomförts.
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		Ja, såvitt är känt har dessa identifierats men konsekvensbedömningar har inte genomförts full ut. Svårt att avgöra. Det har gjorts en översyn och verksamheten ska påbörja arbetet med att konsekvensbedöma behandlingarna i sammanlagt tre ytterligare system.

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.
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		Hittills har det inkommit en (1) begäran om registerutdrag detta år.
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, såvitt kan bedömas.

Personuppgiftsincidenter

Sammanfattning

Incidenthanteringen inom förvaltningen har uppmärksammats i samband med att förvaltningens personuppgiftsbehandlingar har analyserats. Det som kan noteras är att något 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 skickas till fel mottagare. I en ambition att öka antalet rapporterade incidenter kommer verksamheten att dokumentera och följa upp hur många av verksamhetens anställda som genomgår de obligatoriska utbildningarna i informationssäkerhet och dataskydd. Anställda ska även informeras om vanliga typer av incidenter och ges exempel på hur dessa kan undvikas.

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. Regelbunden uppföljning och återkommande samtal i samband med bland annat APT-möten.
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		Ja, såvitt är känt följs gällande rutiner men det finns sannolikt ett behov av att se över rutiner för att underlätta för den som behöver rapportera en incident.
Hur många personuppgiftsincidenter har dokumenterats under året?		Hittills 15 inkl. Miljödata-incidenten. Antalet incidenter har ökat något 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?		Hittills fem incidenter totalt under året.

Överföring till tredje land

Sammanfattning

Flertalet verksamhetssystem som innebär någon form av personuppgiftsbehandling som Kulturförvaltningen 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 de system som förvaltningen har upphandlat och använder i sin verksamhet kan det förekomma överföring av personuppgifter. Det är inte klarlagt i vad mån detta har utretts i tillräcklig utsträckning. Vidare finns det behov av att se över och granska befintliga personuppgiftsbiträdesavtal. Frågan behöver prioriteras.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		Ja, såvitt är känt.
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		Verksamheten stödjer aktuell behandling på gällande adekvansbeslut mellan EU/EES och USA (EU-US DPF).
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		Nej, men verksamheten stödjer aktuell behandling på gällande adekvansbeslut mellan EU/EES och USA (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?

44 behandlingar varav två avser kamerabevakning enligt verksamheten.

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

Ja, såvitt är känt.

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

Delvis. Exempelvis görs endast uppdateringar av systembaserade behandlingar i samband med att avtalen löper ut och nya avtal måste tecknas med leverantörer.

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

Registerförteckningen är huvudsakligen komplett, men det återstår visst arbete med att se över de behandlingar som sker hos leverantörer och underbiträden för att säkerställa att

förvaltningen har aktuella uppgifter av betydelse för verksamhetens efterlevnad av GDPR art. 30.

Dataskyddsombudets jämförelse med föregående års resultat

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

Resultatet är ungefär detsamma som föregående år.

Dataskyddsombudets bedömning samt rekommendationer

Förteckningen bedöms i allt väsentligt vara komplett, men visst arbete återstår med att kontrollera de leverantörer och eventuella underbiträden som utför behandlingen på uppdrag av verksamheten för att identifiera eventuella förändringar som kan ha inverkan på laglighet, säkerhet och lämplighet. 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.

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

Delvis. Här återstår ett arbete för verksamheten att tydligare kommunicera gällande rutiner och styrdokument och att förankra dessa i verksamheten för ett bättre genomslag, inte minst när det kommer till incidenthanteringen.

Dataskyddsombudets jämförelse med föregående års resultat

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

Situationen är ungefär densamma som föregående år.

Dataskyddsombudets bedömning samt rekommendationer

Verksamheten arbetar metodiskt och systematiskt med informationsklassningar. Det finns dock ett behov av att se över andra delar av verksamhetens säkerhetsarbete. Särskilt gäller detta incidenthanteringsprocessen och regelbunden uppföljning av brister i verksamheten.

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, tröskelanalyser genomförs vid nya/förändrade behandlingar. Dessutom genomförs en årlig översyn. Syftet med en tröskelanalys är att metodiskt och strukturerat fånga upp risker som på ett eller annat sätt kan påverka den sammanlagda riskbedömningen utifrån de rättsliga kraven i dataskyddsförordningen. Fördelen med att man i ett initialt skede beaktar dataskyddsrisker är dessutom att man på ett bättre sätt kan fånga upp it-säkerhetsrisker som har betydelse för de mer renodlade dataskyddsriskerna (kopplat till bland annat ändamålsbegränsning, uppgiftsminimering och lagringsminimering). Positivt är att verksamheten genomför tröskelanalyser parallellt med informationsklassning och eventuella it-säkerhetsfrågor för att fånga upp eventuella risker redan i det skedet.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

Ja, såvitt är känt.

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

Delvis. Det saknas ändamålsenliga rutiner. Verksamheten använder dock Integritetsskyddsmyndighetens mall för konsekvensbedömningar.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

Svårt att avgöra. Verksamheten bör göra en översyn av samtliga behandlingar för att kunna utesluta att det förekommer högriskbehandlingar där konsekvensbedömningar behöver genomföras.

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

Ja, såvitt är känt har dessa identifierats men konsekvensbedömningar har inte genomförts full ut. Svårt att avgöra. Det har gjorts en översyn och verksamheten har påbörjat arbetet med att konsekvensbedöma behandlingarna i sammanlagt tre olika system och att därutöver genomföra en konsekvensbedömning för ytterligare ett system.

Dataskyddsombudets jämförelse med föregående års resultat

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

Situationen är ungefär densamma som föregående år.

Dataskyddsombudets bedömning samt rekommendationer

Det återstår ett betydande arbete för verksamheten att se över aktuella behandlingar utifrån kraven på säkerhet och säkerställande av de registrerades rättigheter i enlighet med dataskyddsförordningen.

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, såvitt är känt.

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 [1].

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

Ja, såvitt kan bedömas.

Dataskyddsombudets jämförelse med föregående års resultat

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

Nej, resultatet ligger på samma nivå som föregående år.

Dataskyddsombudets bedömning samt rekommendationer

Verksamheten har, såvitt kan bedömas, ändamålsenliga rutiner och arbetssätt för att hantera olika typer av rättighetsbegäran från registrerade.

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?

I dagsläget oklart i vilken utsträckning verksamheten informerar anställda och säkerställer att anställda har den kunskap som behövs för att veta hur denne ska agera i händelse av en incident.

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

Ja, det finns rutiner.

Hur många personuppgiftsincidenter har dokumenterats under året?

15 incidenter.

Hur många personuppgiftsincidenter har anmälts till IMY under året?

Fem incidenter.

Dataskyddsombudets jämförelse med föregående års resultat

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

Ja, antalet har ökat.

Dataskyddsombudets bedömning samt rekommendationer

Bedömningen är att det finns ett behov av att lyfta vikten av att anmäla misstänkta personuppgiftsincidenter givet det låga antalet rapporterade personuppgiftsincidenter. Det låga antalet beror sannolikt på dels en okunskap kring vad som faktiskt utgör en personuppgiftsincident (i.e. en potentiell risk för den registrerades fri- och rättigheter enligt GDPR), dels vad man ska göra rent praktiskt i händelse av en incident. En komplicerande faktor är att exempelvis en stöld av en mobiltelefon även sannolikt utgör en personuppgiftsincident vilket innebär att incidenten ska rapporteras utifrån flera olika kategorier.

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?

Ja, såvitt kan bedömas.

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?

Verksamheten grundar sådan behandling på EU-kommissionens adekvansbeslut för överföringar av personuppgifter från EU/EES till företag med säte i USA.

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

Nej, verksamheten grundar aktuella behandlingar på ovan nämnda adekvansbeslut.

Dataskyddsombudets jämförelse med föregående års resultat

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

Nej.

Dataskyddsombudets bedömning samt rekommendationer

Givet den tekniska utvecklingen och att allt fler leverantörer väljer att lagra data i molnet ser vi att behovet av såväl tydliga kravställningar som regelbunden uppföljning av leverantörers val av tekniska lösningar och nyttjande av underbiträden blir allt mer påtagligt.

[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 arbetar metodiskt och systematiskt med informationsklassningar. Det finns dock ett behov av att se över andra delar av verksamhetens säkerhetsarbete. Särskilt gäller detta incidenthanteringsprocessen och regelbunden uppföljning av brister i verksamheten. 2. Bedömningen är att det finns ett behov av att lyfta vikten av att anmäla misstänkta personuppgiftsincidenter, tex i APT sammanhang. 3. Givet den tekniska utvecklingen och att allt fler leverantörer väljer att lagra data i molnet ser vi att behovet av såväl tydliga kravställningar som regelbunden uppföljning av leverantörers val av tekniska lösningar och nyttjande av underbiträden blir allt mer påtagligt

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.