Stockholms stad

GDPR årsrapport

År 2025

Servicenämnden

GDPR årsrapport 2025
December 2025

Dnr: SF 2026/105
Utgivningsdatum: 2026-01-22
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
Kontroll och mitigering av risker kopplat till tredjelandsöverföring		Verksamheten bör granska befintliga system och processer för att identifiera samtliga tredjelandsöverföringar som sker för att sedan kunna minimera eventuella risker utifrån typ av behandling och typ av uppgifter.
System och rutiner för rapportering av misstänkta personuppgiftsincidenter		Verksamheten har rutiner för hantering av incidenter. Det finns emellertid behov av att se över behovet av tydligare metodstöd och förenklade arbetssätt. Detta har inte minst kommit att uppmärksammas i samband med Miljödata-incidenten. En bidragande orsak till detta får anses vara att systemstödet IA inte är särskilt ändamålsenligt utformat för hantering av personuppgiftsincidenter.
Tydlighet när det gäller personuppgiftsansvar för att tydliggöra roller och ansvar vid incidenthantering		Här finns ett behov av att se över hur personuppgiftsansvaret är fördelat utifrån dataskyddsregelverket och vilka faktiska förhållanden som föreligger (vem/vilka bestämmer i praktiken ändamål och medel med viss behandling). Detta gäller dels de processer och gemensamma system som kommunstyrelsen samordnar

och svarar för, dels de olika typer av samordning/samverkan som sker mellan serviceförvaltningen och dess kunder (nämnder m.fl.).

Innehållsförteckning

Sammanfattning 1
Inledning 4
Dataskyddsombudets uppgift 4
Granskning av dataskyddsarbetet 5
Kontroll av sex obligatoriska områden 5
Resultat från granskningen av de sex obligatoriska områdena 6
Register över personuppgiftsbehandlingar 6
Säkerhet i samband med behandlingen 8
Konsekvensbedömning avseende dataskydd 9
Den registrerades rättigheter 10
Personuppgiftsincidenter 12
Överföring till tredje land 13
Bilagor 15
Bilaga 1 - Detaljerad redovisning av dataskyddsombudets granskning ... 16
Bilaga 2 – Rekommendationer och omvärldsbevakning 25

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 sex 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

Antalet registrerade behandlingar överstiger 1000 vilket kan göra det svårt att få en snabb överblicksbild. Verksamheten anser emellertid att detta förfarande underlättar i arbetet, och ger en mer heltäckande bild över vilka personuppgifter som behandlas i respektive process, såtillvida att hanteringsanvisningarna och behandlingsregistret finns samlat i ett och samma dokument/register. Detta förhindrar dock inte att man redovisar detta på en aggregerad nivå i andra sammanhang eller i pedagogiskt syfte.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		Det finns totalt 1045 behandlingar registrerade i registerförteckningen i VisAlfa räknat på handlingstyp.
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		Ja.
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		Delvis. Vad gäller de centrala system som Kommunstyrelsen upphandlar och kravställer genom Stadsledningskontoret, och som används av Serviceförvaltningen, finns en viss osäkerhet kring huruvida eventuell tredjelandsöverföring av personuppgifter förekommer i dessa system. Denna osäkerhet bör adresseras än mer och stämmas av regelbundet i samråd med

		Kommunstyrelsen (genom Stadsledningskontoret).
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)?		Samma som ovan.

Säkerhet i samband med behandlingen

Sammanfattning

Iakttagelsen 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 något oklart hur de bör hänga ihop. Det pågår ett arbete internt med att se över detta och det kan vara lämpligt att även verksamhetens dataskyddsombud lämnar rekommendationer och förslag på förbättringar.

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 hänsyn till olika kategorier av personuppgifter.
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.

Konsekvensbedömning avseende dataskydd

Sammanfattning

Flertalet konsekvensbedömningar har gjorts inom ramen för bland annat rekryteringsprocessen/hanteringen. Förnyade bedömningar görs dock inte löpande. Det saknas idag förutsättningar för detta då de olika verksamheterna inte alltid informerar serviceförvaltningen om nya behandlingar (nya arbetssätt, lokala upphandlingar).

Föreslagna säkerhetsåtgärder bör följas upp löpande. Det finns också anledning att granska vissa behandlingar närmare i ljuset av den senaste tidens incidenter som berott på tekniska sårbarheter såväl som bristande rutiner och bristande kontroll.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		Det finns mallar (staden/lokalt). Verksamheten har godtagbara rutiner som stöd i upphandlingsverksamheten och därmed stadens övriga förvaltningar vid upphandlingar. Verksamheten har även fått med tröskelanalys och konsekvensbedömning i de processkartor som beslutats av FL (för både A, B- och C-klassning och som även redovisats på chefsforum), och i hanteringen av årliga klassningar finns det även med som check-punkt. Verksamheten har tagit fram ett utkast till rutin.
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		Ja, men det kan finnas skäl att se över detta inom Kontaktcenter Stockholm, närmare bestämt när de får nya uppdrag som innebär nya personuppgiftsbehandlingar och ofta med kunder som kanske inte själva har fullständig insikt och kunskap kring detta. Vidare kan ökad användning av AI sannolikt föranleda fördjupade analyser i vissa fall.
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 bistår verksamheten och kan vid behov leda möten och stötta i dokumentation samt lämna förslag på vad som bör prioriteras.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		Såvitt känt, ja. Situationen har förbättrats avsevärt jämfört med föregående år. Inom verksamheten har det emellertid uppmärksammats att det inom Kontaktcenter Stockholm finns ett behov av att arbeta mer strukturerat i dessa frågor. Värt att notera är att en del av Kontaktcenter Stockholms behandlingar kommer att konsekvensbedömas inom ramen för upphandlingen av nytt ärendehanteringssystem. Detta är positivt. Värt att tillägga är att ökad användning av AI sannolikt kan föranleda fördjupade analyser i vissa fall.
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 ramen för rekryteringsprocessen. Det finns en referenskonsekvensbedömning från SLK som gäller personuppgifter i personalsystem. Vidare konsekvensbedöms stora delar av förvaltningens behandling av känsliga personuppgifter inom ramen för upphandlingen av ett nytt ärendehanteringssystem.

Den registrerades rättigheter

Sammanfattning

Under 2025 har informationen till registrerade uppdaterats på stadens hemsida stockholm.se och information riktad till anställda finns nu 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?		Verksamheten har rutiner för registerutdrag och radering, men saknar rutiner för information, rättelse, invändning och begränsning.

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

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.

De vanligaste incidenterna är att e-postmeddelanden skickas till fel mottagare eller att det sker misstag vid manuell inmatning av personuppgifter i verksamhetens olika system.

Serviceförvaltningen arbetar för närvarande med att se över rutinerna för verksamhetens incidenthantering. Här är förvaltningens ISAM drivande i arbetet. Även verksamhetens dataskyddsombud är aktivt involverade i detta arbete.

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?		Detta säkerställs genom information på Intranätet och förvaltningens samarbetsyta med mallar för hur incidenterna ska hanteras. Vidare gås incidenthanteringsprocessen igenom regelbundet med särskilt fokus på personuppgiftsincidenter, flera avdelningar har utvecklat eller jobbar med att ta fram egna rutiner. Förvaltningen avser också att ta fram en gemensam incidenthanteringsrutin under det fjärde kvartalet av 2025 (senast under det första kvartalet 2026) som sedan kommer att förmedlas till anställda via en förvaltningsövergripande utbildning i informationshantering.
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		Det finns rutiner för detta, men dessa behöver sannolikt ses över givet det låga antalet rapporterade incidenter internt i förvaltningen. Vissa upplever incidenthanteringsprocessen som krånglig.
Hur många personuppgiftsincidenter har dokumenterats under året?		Hittills 104 stycken varav fyra i egenskap av personuppgiftsansvarig (2025-11-21).

		Antalet rapporterade incidenter har ökat sedan förra årets redovisning. Ökningen kan främst förklaras med att fler incidenter rapporteras via IA och därför blir kända.
Hur många personuppgiftsincidenter har anmälts till IMY under året?		En (1) incident.

Överföring till tredje land

Sammanfattning

Flertalet verksamhetssystem som innebär någon form av personuppgiftsbehandling som serviceförvaltningen använder är system som tillhandahålls centralt. Utgångspunkten har därför varit att granskning av och bedömning kring eventuell överföring till tredje land har gjorts i samband att systemen upphandlats och införts. Vad gäller de lokalt upphandlade systemen sker denna bedömning i förekommande fall hos Serviceförvaltningen.

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		Svårt att avgöra helt säkert då förvaltningen delvis använder centrala system och där finns viss osäkerhet kring huruvida Stadsledningskontoret löpande fullt ut informerar om alla förändringar som sker hos leverantörer och underbiträden och som är av betydelse för frågan om tredjelandsöverföring. Vidare är det svårt för serviceförvaltningen att kontrollera huruvida stadsledningskontoret fullt ut har beaktat och kontrollerat leverantörernas och deras underbiträdens tekniska lösningar och eventuella förändringar i leverantörskedjor och teknisk infrastruktur.
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		Verksamheten stödjer sina tredjelandsöverföringar 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, men enligt dataskyddsförordningen krävs det inte uttryckligen att en bedömning (TIA) genomförs för alla behandlingar som innebär tredjelandsöverföring.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

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?

1045 behandlingar finns registrerade i förvaltningens IT-stöd för hanteringsanvisningar och behandlingsregister VisAlfa.

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

Inom klassificeringsmodellen för upphandling av nya system används metodstödet KLASSA för att klassa den information som ska behandlas. Det finns en handlingsplan som beskriver uppdatering av registerförteckning, likaså i klassningsbeskrivningen. Klassa används inte enbart för informationsklassningar i samband med upphandlingar utan också för nya och befintliga behandlingar generellt. Klassa används för bedömning av processer och information. Det faktum att Klassa-modellen utgår från systembaserade behandlingar bidrar emellertid att processen kan framstå som något ologiskt utifrån ett rent dataskyddsperspektiv. Det åligger ansvarig chef att säkerställa att hanteringsanvisningar är ändamålsenliga och uppdaterade.

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

Uppdateringar sker en gång per år i samarbete med registrator och verksamheterna. Uppföljningsrutin finns enligt årshjul hos registrator. Uppdateringar sker löpande av

registratur vid kända förändringar. Inventering, som leds av registrator, sker tillsammans med verksamheterna en gång per år.

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

Ja, delvis. Vad gäller de centrala system som Kommunstyrelsen svarar för att upphandla och kravställa genom Stadsledningskontoret, och som används av Serviceförvaltningen, finns en viss osäkerhet kring huruvida eventuell tredjelandsöverföring av personuppgifter förekommer i dessa system.

Dataskyddsombudets jämförelse med föregående årsresultat

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

Föregående granskning menar att registret är för omfattande och innehåller för många poster för att kunna granskas.

Dataskyddsombudets bedömning samt rekommendationer

I ett svar från verksamheten anges att det skulle behövas förbättringar om hur verksamheten själva initierar förändringar som påverkar behandlingsregistret. Man uppger att det finns vissa brister såvitt avser lokala rutiner/arbetssätt. Problematiken består i att registraturen ibland inte får information från bl.a. Kontaktcenter Stockholm om nya uppdrag eller tjänster. Detta gäller mindre såväl som större upphandlingar eller när vissa uppdrag upphör. I bästa fall upptäcks nya eller förändrade uppdrag i samband med den årliga inventeringen. Med anledning av detta bör framför allt Kontaktcenter se över sina rutiner och processer för att säkerställa att registerförteckningen uppdateras i takt med att det tillkommer eller försvinner behandlingar i verksamheten.

Verksamheten har genomfört en processklassning i samband med att nytt ärendehanteringssystem ska upphandlas, och har därigenom fångat in inom vilka processer i hanteringsanvisningarna som behöver uppdateras och samtidigt kunnat lyfta betydelsen av dem.

I övrigt bör nämnas att det i verksamhetens nya system för informationshantering VisAlfa finns en teknisk lösning för att dela ut ”projekt” till verksamheterna i VisAlfa så att de själva kan föreslå/påverka/påtala förändring av innehållet i registret. Att arbeta på detta sätt skulle dock kräva insatser i form av utbildning etc. I skrivande stund har denna funktion ännu inte aktiverats.

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 gjorda 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

En stickprovskontroll har valts ut, utifrån registerförteckning och hanteringsanvisningar för känsligare processområden. Kontroll har gjorts för Artvise som är det verktyg som används för ärendehantering inom verksamheterna.

Serviceförvaltningens klassningsdokument visar tydligt att informationen är av högt skyddsvärde. Det finns en lista över implementerade skyddsåtgärder. Informationsägarskapet framgår vad gäller de klassningar som görs i stadens centrala och gemensamma upphandlingar är dock inte alltid tydligt. Detta är något som bör ses över och följas upp.

Informationsägarskapet avser de som ska använda avtalet. Detta finns inte alltid uttryckligt angivet i själva klassningsprotokollet i exempelvis centrala upphandlingar. Det kan därför finnas en poäng i att tydliggöra detta förhållande i klassningsprotokollet eller på annat sätt så att detta blir tydligt. Vanligt förekommande är att det i stället för att vara tydligt angivet står något i stil med *nyttjande förvaltning eller bolag*.

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

De skriftliga styrande dokumenten för dataskydd följer stadens mallar och kompletteras med egna lokala anvisningar, rutiner för hantering av personuppgiftsincidenter, hantering för begäran om radering och registerutdrag. Dessa är publicerade och tillgängliga på en samarbetsyta på intranätet, samt håller god kvalité. Även vid central kravställning är det viktigt att ta hänsyn till lokala krav i de olika förvaltningarna eftersom det är där behandlingarna sker.

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

Överlag har Serviceförvaltningen bra dokumentation och rutiner. Det finns dock ett behov av att se över organisationen för dataskydd med anledning av den omfattande mängden uppdrag och processer som förvaltningen projektleder och upphandlar åt andra förvaltningar i kommunen.

Dataskyddsombudets jämförelse med föregående års resultat

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

Verksamheten har en handlingsplan för förvaltningens arbete som har tagits fram inom ramen för funktionsarbetet. Det saknas emellertid en tydlig handlingsplan avseende Artvise. Detta är väsentligt för att vi ska kunna få en helhetsbild avseende de bedömningar som gjorts gällande säkerhet för systemet. Artvise innehåller all känslig data som finns i kundtjänstsystem.

Dataskyddsombudets bedömning samt rekommendationer

Bedömningen är att verksamheten överlag arbetar strukturerat och metodiskt med dessa frågor. Verksamheten har utvecklat sitt säkerhetsarbete sedan föregående år. En starkt bidragande orsak till detta är att detta prioriteras på ett annat sätt än tidigare, att förvaltningens ISAM fått en mer framträdande roll och att samarbetet mellan ISAM och dataskyddshandläggare har intensifierats.

3. Konsekvensbedömning avseende dataskydd

Bakgrund och syfte

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

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

Genom att genomföra en konsekvensbedömning kan personuppgiftsansvarig identifiera risker med en personuppgiftsbehandling, hantera riskerna genom åtgärder och rutiner samt påvisa ansvarsskyldighet. Genom konsekvensbedömningar kan risker identifieras och förebyggas.

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

Kontroller och iakttagelser gjord av dataskyddsombudet

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

Serviceförvaltningen använder sig av stadens klassningsrutin, och dels egna metodstöd /mallar för tröskelanalyser.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

Det finns ett förbättringsbehov framför allt inom Kontaktcenter Stockholm, som när de får nya uppdrag som innebär nya personuppgiftsbehandlingar, och ofta med kunder som kanske inte själva har fullständig koll.

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

Staden har tagit fram mallar, IMYs mallar har också använts av förvaltningen. DSO rekommenderar att man använder IMYs mall, men att nya mallar från staden också kan användas förutsatt att de innehåller de delar som IMY rekommenderar. Tidigare mallar från staden saknade tydlig riskanalys, samt plats för DSOs råd och rekommendationer.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

Där tröskelanalys har visat att konsekvensbedömningar ska genomföras, är de i process att genomföras eller har genomförts.

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

Förvaltningen har inte genomfört en tröskelanalys av samtliga behandlingar.

Dataskyddsombudets jämförelse med föregående års resultat

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

Verksamheten befinner sig i ungefär samma läge som förra året om inte bättre (grön nivå).

Dataskyddsombudets bedömning samt rekommendationer

Den sammanlagda bedömningen är att verksamheten har en hög medvetenhet kring dessa frågor och arbetar strukturerat med att identifiera högriskbehandlingar som kräver att konsekvensbedömningar görs. Verksamheten har erforderlig kompetens för att hantera detta. Vad gäller de centralt upphandlade systemen föreligger emellertid en viss osäkerhet eftersom förvaltningen inte har samma kontroll över processen och de bedömningar som gjorts kopplat till risker och säkerhet. Med anledning av detta behöver verksamheten sannolikt vara än mer delaktig i de centrala processerna, genom de s.k. referensgrupperna, med större fokus personuppgiftshantering och dataskydd.

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?

Förvaltningen har tagit fram rutiner för att hantera begäran om radering och begäran om registerutdrag. Båda är rutiner med hög kvalité och enligt lagstiftning. Dock innehåller mallen för registerutdrag information som skulle kunna ses som otillräcklig och leda till oklarheter vid utskick. Det är viktigt att man i informationen även informerar den registrerade om hur länge informationen ska bevaras, samt tredjelandsöverföring. Då förvaltningen även arbetar med profilering i samband med rekrytering ska informationen om kriterier och systematik tydligt framgå i ett registerutdrag. Även detta bör ingå i mall. Det finns ingen skriftlig rutin för hantering av rättelse, begränsning, invändning och förflyttning (dataportabilitet).

Serviceförvaltningen har med information om förvaring (alltså vilka system som används) i mallen för registerutdrag. Det är inte nödvändigt – upp till er om ni vill inkludera det eller inte. Det påverkar inte regelefterlevnaden – varken till eller från. Kan normalt finnas säkerhetsrisker med det men det är ofta ändå offentligt för offentlig förvaltning. Det kan vara värt att notera att även loggar kan vara nödvändigt att ta ut (dvs. att någon sett information).

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

2 stycken begäranden om radering (föregående år 3 stycken). Ingen av dessa begäranden har beviljats.

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

Samtliga (samma som föregående år).

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

Ja, såvitt kan bedömas i efterhand uppfyller svaren de krav som framgår av regelverket.

Dataskyddsombudets jämförelse med föregående års resultat

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

Inga nämnvärda avvikelser jämfört med föregående år.

Dataskyddsombudets bedömning samt rekommendationer

Förvaltningen föreslås komplettera rutinen för hantering av begäran till att även innefatta andra rättigheter såsom hur man hanterar begäran om dataportabilitet, ändring, invändning m.m.

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.

Även om en personuppgiftsincident inte bedöms vara anmälningspliktig ska den dokumenteras då samtliga personuppgifter ska 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?

Förvaltningens medarbetare ska genomföra stadens utbildningar i utbildningsportalen. Detta följs upp årligen en gång per år av ISAM. Information om utbildningar har getts senast vid chefsforum 2024.

Dataskyddshandläggare och ISAM informerar särskilt om enheterna önskar, och detta har skett vid ett tillfälle under året. Rutiner för hantering av personuppgiftsincidenter finns tillgängliga på förvaltningens samarbetsyta. De följer stadens centrala rutiner men med komplettering av information. Serviceförvaltningen är unik i sin roll som biträde för samtliga stadens nämnder, inom flera områden, vilket innebär utökat ansvar för att rapportera och ha kontroll över personuppgiftsincidenter men där det ankommer på personuppgiftsansvarig nämnd att faktiskt anmäla till tillsynsmyndighet. Medarbetare på förvaltningen uppger att det alltid finns behov av att stärka medvetenheten kring rutiner, då tidsaspekten inte alltid följts och en viss osäkerhet har funnits kopplat till incidenthanteringsprocessen och som det pågår en översyn av. Det är inte helt klarlagt vad denna osäkerhet består av, men den preliminära slutsatsen är att det sannolikt krävs ytterligare insatser i form av utbildning eller dragningar på APT-möten eller liknande. Av erfarenhet kan sägas att konkreta exempel på incidenter och hur dessa bör hanteras generellt sett ger bäst effekt eftersom dataskyddsfrågor annars kan te sig teoretiska och svåra att greppa.

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

Se ovan.

Hur många personuppgiftsincidenter har dokumenterats under året?

Per den 21 november 2025 finns totalt 104 registrerade personuppgiftsincidenter varav 4 av dessa ligger under Servicenämndens personuppgiftsansvar. Föregående år var antalet 25 respektive 2.

Hur många personuppgiftsincidenter har anmälts till IMY under året?

1 incident [incident hos Miljödata]. Föregående år gjordes ingen anmälan.

Dataskyddsombudets jämförelse med föregående års resultat

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

Förra året hade grönt i sin rapport. Serviceförvaltningen står alltjämt ut som ett gott exempel på där man har arbetat aktivt med frågan.

Dataskyddsombudets bedömning samt rekommendationer

Serviceförvaltning har arbetat aktivt med personuppgiftsincidenter och uppföljningar, men själva noterat en viss fördröjning för rapportering av personuppgiftsincidenter och viss okunskap om såväl rutiner som begrepp enligt dataskyddsförordningen. En sådan uppföljning tyder på en högre mognadsgrad hos förvaltningen inom området, där inte bara enskilda incidenter följs upp utan även noterar tendenser.

Rutinerna hanterar främst rapporteringskedjan för incidenter men inte hanteringskedjan gällande omedelbara åtgärder och åtgärder för att säkra bevis vid incidenter. Föreslår att rutinen kompletteras med dessa delar.

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?

Förvaltningen uppger att man inte säkert kan säga att man identifierat alla tredjelandsöverföringar. Detta gäller stadens centrala system. En oklarhet i personuppgiftsansvar kan ses som delorsak till detta, mellan stadens nämnder, mellan Kommunstyrelsen, serviceförvaltningen och övriga nämnder. Vidare finns viss osäkerhet kring huruvida Stadsledningskontoret fullt ut har beaktat och kontrollerat leverantörernas och

[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.

deras underbiträdens tekniska lösningar såsom förändringar i leverantörskedjor och teknisk infrastruktur.

För de system där nämnden själv är informationsägare har dock noteringar gjorts i behandlingsregister och PuB-avtal för de behandlingar där tredjelandsöverföring förekommer.

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?

I de tredjelandsöverföringar som noterats och är utredda, gäller standardavtalsklausuler. Vidare kan konstateras att verksamheten i enlighet med gällande adekvansbeslut kan överföra personuppgifter till USA under förutsättning att mottagarna omfattas av EU-US Data Privacy Framework. Detta adekvansbeslut gäller alltjämt, men det finns en betydande risk för att detta beslut inte står sig för evigt varför verksamheten bör ha beredskap för detta och ha överföringsverktyg och/eller exitstrategier på plats.

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

Verksamhetens tredjelandsöverföringar omfattas av EU-kommissionens adekvansbeslut varför TIA inte bedömts nödvändigt.

Dataskyddsombudets jämförelse med föregående års resultat

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

Detta område är nytt i och med denna årsrapport.

Dataskyddsombudets bedömning samt rekommendationer

Oavsett om personuppgiftsansvaret är delat eller om man enbart är biträde måste tredjelandsöverföringar vara noterade. Avsaknad av kontroll för tredjelandsöverföring och inventering av att sådana är gjorda är en allvarlig brist. Förvaltningen bör gå igenom samtliga behandlingar för att identifiera tredjelandsöverföringar där sådana finns. Rekommendationen är att, i de fall verksamheten inte kan garantera en säker överföring av personuppgifter, upphöra eller pausa överföringen och genomföra en Transfer Impact Assessment (TIA) där överföringsverktyget är s.k. standardavtalsklausuler SCC. Dels bör stadsledningskontoret fastställa vad som gäller för de centrala systemen, dels bör enskilda verksamheter (kunder) kunna redogöra för detta såvitt avser de lokala system som används inom förvaltningen.

Bilaga 2 – Rekommendationer och omvärldsbevakning

Dataskyddsombudets rekommendationer baserat på iakttagelserna ovan

Dataskyddsombudets rekommendationer
1. *Förvaltningen bör fortsätta sitt arbete med att utöka sin organisation för dataskyddsarbete. Särskilt betonas vikten av vidareutbildning och resursstöd för upphandlingsområdet gällande dataskydd,* 2. *Nämnden bör lägga ännu mera fokus på att kontrollera befintliga processer och behandlingar och säkerställa att dessa har lagligt stöd i sin helhet samt att det för högriskbehandlingar genomförs konsekvensbedömningar i de fall detta inte redan har gjorts. I de fall det skulle saknas laglig grund kan verksamheten behöva upphöra med viss behandling eller åtminstone pausa behandlingen, och utföra den först om det framkommit att den kan genomföras.*

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.

Övrigt att rapportera

Rapport särskilt från dataskyddsombud under perioden 1 mars till 12 september:

Tidigare dataskyddsombud har påpekat problematiken kring stadens fördelning av personuppgiftsansvar. Frågan kvarstår för stadens nämnder och i relation till Kommunstyrelsen. Det har visat sig problematiskt både vad gäller uppföljningar och vid personuppgiftsincidenter, där ansvarsskyldigheten riskeras. Det bidrar till en otydlighet såtillvida att det kan vara svårt att veta vem som bär huvudansvaret för vissa åtaganden kopplat till personuppgiftsbehandlingar.

Enligt stadgar för nämnderna ska en instruktion eller annan beskrivning göras om det råder en personuppgiftsbiträdes-relation eller ett delat personuppgiftsansvar. Sådana instruktioner saknas.

Personuppgiftsansvaret bör som utgångspunkt följa på det ansvar som de självständiga myndigheterna inom staden har för att fatta beslut. Nämndernas uppdrag följer på beslut från kommunfullmäktige. När t.ex. beslut tas om gemensam IT eller gemensamma IT-system, där enskilda nämnder har att ingå i dessa, bör det därför också vila ett visst personuppgiftsansvar på den nämnd som fått det uppdraget att införa dessa. En nämnd bör alltså bara ha ett personuppgiftsansvar inom kommunen för den behandling av personuppgifter som de faktiskt kan påverka. När personuppgiftsbehandlingen sker på grund av dessa sammanlänkande beslut kan ett gemensamt personuppgiftsansvar inträda. Förvaltningen bör gemensamt med främst

stadsledningskontoret kräva förtydligande för personuppgiftsansvaret där nämnden inte har beslutanderätt för hela behandlingen utan bara delar av den.