Stockholms stad

GDPR årsrapport

År 2025

Kulturhuset Stadsteatern

GDPR årsrapport
Januari 2025

Dnr: KHST 2026/14
Utgivningsdatum: 2025-01-16
Kontaktperson: Petra Kanon

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 Kulturhuset Stadsteaterns dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

I rapporten konstateras att KHST bedriver ett dataskyddsarbete som håller god nivå och som kontinuerligt utvecklas men att vissa förbättringsområden finns. Ett av dessa förbättringsområden är även detta år verksamhetens kunskap gällande personuppgiftsincidenter som bedöms vara bristfällig, vilket mest troligt förklarar den låga frekvensen av inrapporterade personuppgiftsincidenter. Överlag förbättras emellertid dataskyddsarbetet löpande och i år har förbättringar skett inom arbetet med konsekvensbedömningar.

Den samlade risknivån bedöms som acceptabel.

De största riskerna enligt dataskyddsombudets bedömning

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
Kunskap kring incidenter	🟡	*Fortsätt med de riktade utbildningarna för att säkerställa en tillräcklig kunskapsnivå.*
Hantering av registrerades rättigheter	🟡	*Gör stickkontroller hos kundtjänst för att säkerställa att hanteringen är korrekt.*
Personuppgiftsberoende	🟡	*Utveckla en dataskyddsorganisation där verksamheten tar större ansvar.*

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 2025

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.

Resultatsammanställning och centrala iakttagelser inom dataskyddsarbetet

I detta avsnitt presenteras en sammanställning av den bedömda risknivån för verksamhetens dataskyddsarbete, grundat på kontrollfrågorna inom de sex obligatoriska områdena. Vidare redovisas 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

Antal behandlingar bedöms rimliga och spegla de behandlingar som sker i verksamheten. Rutiner finns för att hålla registret uppdaterat. På det stora hela håller registret och hanteringen av det en bra nivå. Verksamheten bör dock ta ett större ansvar för hanteringen.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		76 behandlingar är registrerade.
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		Rutiner finns som är ändamålsenliga.
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		Rutiner finns men bedömningen är att verksamheten inte är tillräckligt medveten om kraven, vilket innebär att registrering och uppdatering till stor del sköts av dataskyddssamordnare och informationssäkerhetssamordnare. Rekommendationen är att ledningen klargör ansvaret för verksamheten inom detta område.

Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		De har i stor utsträckning besvarats men informationen anses i vissa fall inte vara korrekt vad gäller angivande av rättslig grund. Rekommendationen är att förbättra kvalitén på innehållet i registreringarna

Säkerhet i samband med behandlingen

Sammanfattning

Det finns ändamålsenliga styrdokument på plats och arbetet med informationssäkerhet håller en bra nivå utifrån verksamhetens behov.

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?		Bedömningen är att informationsklassningarna i tillräcklig utsträckning tar hänsyn till personuppgifter men att metoden att informationsklassa utifrån system kan innebära en risk. Verksamheten har bra rutiner för området och rekommenderas att fortsätta med det systematiska arbetet.
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		Styrdokumenten på området anses ändamålsenliga. Rekommendationen är att fortsätta det systematiska arbetet med styrdokument.
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		Bedömningen är att verksamheten inte har tillräcklig kunskap inom området och rekommendationen är att ledningen klargör vikten av dataskydd.

Konsekvensbedömning avseende dataskydd

Sammanfattning

Verksamheten har rutiner för att identifiera när konsekvensbedömningar behöver göras. En ny mall har införts som bedöms förbättra kvaliteten på konsekvensbedömningarna. Tidigare genomförda konsekvensbedömningar är innehållsmässigt och kvalitetsmässigt inte tillräckliga.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		Ändamålsenliga rutiner och styrdokument finns på plats. Rekommendationen är att fortsätta det systematiska arbetet med styrdokument.
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		I och med den nya mallen genomförs tröskelanalyser. Rekommendationen är att fortsätta det systematiska arbetet med styrdokument.
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		Mall och rutiner finns. Rekommendationen är att fortsätta det systematiska arbetet med styrdokument.
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		Konsekvensbedömningar genomförs men bedömningen och rekommendationen sedan tidigare är att de innehållsmässigt inte håller tillräcklig kvalité. Dock är bedömningen att detta kan komma att förbättras i och med den nya mallen.
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		I stor utsträckning är bedömningen att de behandlingar som kräver en konsekvensbedömning är identifierade men rekommendationen är fortsatt att göra en tröskelanalys gällande biblioteksverksamheten.

Den registrerades rättigheter

Sammanfattning

Med anledning av att statistik eller stickprovskontroller inte görs är det svår att göra några säkra uttalanden. Rekommendationen är att detta följs upp av antingen verksamheten eller att dataskyddsombudet gör en granskning av kundtjänst hantering av begäran om radering och rättelse.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	**Risk**	**Rekommendationer**
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		Majoriteten av begäran hanteras av kundtjänst löpande. Det förs ingen statistik så frågan kan inte besvaras.
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		Majoriteten av begäran hanteras av kundtjänst löpande. Det förs ingen statistik så frågan kan inte besvaras.
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		Majoriteten av begäran hanteras av kundtjänst löpande. Det förs ingen statistik så frågan kan inte besvaras.
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		Majoriteten av begäran hanteras av kundtjänst löpande. Det förs ingen statistik så frågan kan inte besvaras.

Personuppgiftsincidenter

Sammanfattning

Anmälda incidenter är få men de som anmäls hanteras korrekt. Vid granskning av verksamheten är uppfattningen att hanteringen av personuppgifter främst sker inom administrativa delen (främst HR och kundtjänst) och att kunskapen kring hantering av personuppgifter är varierande hos de som arbetar inom dessa områden. Det finns anledning att misstänka ett visst mörkertal men utbildning sker kontinuerligt.

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?		Utöver styrdokument och information på intranätet genomför dataskyddsamordnaren riktade utbildningar. Rekommendationen är att de riktade utbildningarna bör fortsätta eftersom bedömningen är att det finns risk för att inte alla incidenter anmäls med hänsyn till det låga antalet anmälda personuppgiftsincidenter.
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		Styrdokument och rutiner finns och bedöms följas när dataskyddssamordnare och informationssäkerhetssamordnare får information om eventuell incident. Risken som identifierats är att verksamheten på grund av kunskapsbrist möjligen inte rapporterar in alla eventuella incidenter och därmed följs inte rutinerna.
Hur många personuppgiftsincidenter har dokumenterats under året?		Fyra stycken.
Hur många personuppgiftsincidenter har anmälts till IMY under året?		Inga anmälda incidenter har ansetts vara av så allvarlig att anmälan till IMY har krävts.

Överföring till tredje land

Detta område är ett nytt obligatoriskt granskningsområde för år 2025. DSO har inte genomfört några särskilda granskningar kring denna fråga och har därför inte tillräckligt med underlag för bedömningarna. Rekommendationen är att denna fråga granskas 2026.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		Någon närmare granskning har inte gjorts men rutiner finns på plats för att hantera frågan vid bland annat upphandling.
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		Rutiner finns för att bedöma vad för slags överföringsverktyg som kan behövas men närmare granskning eller stickprovskontroller har inte gjorts.
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		Rutiner finns för att bedöma vad för slags överföringsverktyg som kan behövas men närmare granskning eller stickprovskontroller har inte gjorts.

Bilagor

Bilaga 1: Detaljerad redovisning av dataskyddsombudets granskning

Bilaga 2: Andra genomförda granskningar och omvärldsbevakning

Bilaga 1 - Detaljerad redovisning av dataskyddsombudets granskning

Denna bilaga innehåller en beskrivning av syftet med respektive obligatoriskt område samt en mer detaljerad redovisning av dataskyddsombudets 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?

Det finns 76 behandlingar registrerade i Draftit, vilket är samma som förra året. Dock har vissa justeringar gjorts under året där vissa behandlingar har slagits samman och vissa behandlingar brutits ut.

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

Ja. Uppdateringar sker systematiskt en gång per år samt löpande vid behov.

Dataskyddssamordnare och informationssäkerhetssamordnare håller ihop arbetet och tar huvudansvaret för att uppdateringar genomförs.

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

Enligt rutin sker uppdatering en gång per år samt löpande vid behov. Bedömningen är att denna rutin följs och nödvändiga uppdateringar sker därför i den omfattning som krävs.

Vid kontroll i Draftit har uppdateringar skett under främst september 2025. DSO noterar i år att det finns vissa behandlingar som inte har uppdaterats sedan 2022.

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

Ja.

Dataskyddsombudets jämförelse med föregående års resultat

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

Resultatet är i stor utsträckning densamma som förra året på så vis att KHST arbetar systematiskt med frågorna och ständiga förbättringar sker (även om det är fortsatt personbundet).

Dataskyddsombudets bedömning samt rekommendationer

Den övergripande bedömningen är samma som förra året. Registerförteckningen bedöms vara fullständig på så vis att antal behandlingar och arten av behandlingar får ses som adekvata och relevanta med hänsyn till verksamhetens storlek och inriktning.

Likt de två senaste årsrapporterna noterar dataskyddsombudet att vissa behandlingar bör kontrolleras gällande rättsliga grunden *avtal* som bedöms användas för behandlingar där den grunden inte är tillämplig.[1]

DSO noterar också att för behandlingen personalärenden har det uppgetts att uppgifter om brott behandlas. KHST har rutiner för att kontrollera belastningsregister kopplat till personer som arbetar med barnskådespelare och uppger att rutinen följer gällande rätt. Den notering som görs är att det endast noterat att kontroll mot belastningsregister har gjorts. DSO har inga kommentarer på ett sådant förfarande.

DSO har i år följt upp frågan om att samtycke används som rättslig grund i anställningsförhållanden. Dataskyddssamordnaren har uppgett att samtycke används för publiceringar på sociala medier och en bedömning och konsekvensbedömning har gjorts att detta är den lämpliga rättsliga grunden för denna behandling. Om situationen är sådan för de anställda att det står klart att det är frivilligt, att samtycket går att återkalla och de anställd får den information de har rätt till anser DSO att detta kan vara en av de undantagssituationer där samtycke för anställda går att använda.

Som stöd för att registrera personuppgiftsbehandlingar finns *Vägledning – Inventering av personuppgifter* från Stockholm stad samt en hanteringsanvisning. Enligt hanteringsanvisningen är det enhetscheferna, eller personer utsedda av enhetscheferna, är ansvariga för att lägga in och uppdatera behandlingar som rör deras verksamhet och dataskyddssamordnare kontrollerar och godkänner sedan registreringarna.

---

[1] Följande behandlingar ingick i stickprovet: administration av IT-system, avtalsförvaltning, fackliga förhandlingar/kontakter, personalärenden samt upprättande av styrelsehandlingar och protokoll etc.

Dataskyddsamordnaren har också kontakt med de ansvariga för behandlingarna och påminner om att kontrollera att behandlingarna är aktuella och korrekta. I realiteten är det emellertid dataskyddssamordnaren och informationssäkerhetssamordnaren som får göra uppdateringarna.

Både riktade utbildningar samt e-utbildningar har hållits under året där bland annat information om registerförteckningar finns med.

Bedömningen är att det finns lämpliga rutiner och strukturer på plats men att utmaningen är att se till att de tillämpas ute i verksamheten och att verksamheterna tar sitt ansvar att uppdatera och registrera behandlingar.

Risken som DSO kan notera även tidigare år är att upprätthållandet av registerförteckningen är personberoende, vilket som utgångspunkt inte är lämpligt. Även fast informationsägare har ett ansvar för sina behandlingar är det likväl till stor del dataskyddssamordnaren och informationssäkerhetssamrodnaren som upprätthåller arbetet.

De identifierade bristerna som är värd att nämna är behandling av uppgifter om brott, de fem utvalda behandlingar som har avtal som rättslig grund samt de behandlingar som inte har uppdaterats sedan 2022. Dessa bör ses över. Det är dock relativt enkelt och går snabbt att åtgärda. De övriga identifierade bristerna rör framför allt att förbättra innehållet i redan inlagda behandlingar. Med hänsyn till att verksamheten har ett fortlöpande arbete med dataskyddsfrågor, har en registerförteckning som håller en god kvalitet och att de brister som identifierats främst handlar om förbättringar är bedömningen dock att risken är låg.

Personuppgiftsansvarige bör fortsätta att fokusera på att öka kvaliteten av innehållet i registerförteckningen. Det är även rekommenderat att se till att verksamheten tar sitt ansvar för att uppdatera och registrera personuppgiftsbehandlingar.

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.

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?

Nej.

Dataskyddsombudets jämförelse med föregående års resultat

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

Resultatet är i stor utsträckning densamma som förra året på så vis att KHST arbetar systematiskt med frågorna och ständiga förbättringar sker (även om det är fortsatt personbundet).

Dataskyddsombudets bedömning samt rekommendationer

Styrdokument

De styrdokument som är upprättade bedöms uppfylla kraven för att verksamheten ska kunna jobba systematiskt med dataskydd. Det finns styrdokument med grundläggande information om personuppgiftsbehandling samt mer riktade styrdokument för särskilda områden.

Gällande hantering av känsliga personuppgifter inom HR har DSO fått information om en rutin nu finns på plats.

Uppdateringar har skett av lokal anvisning informationssäkerhet, lokal anvisning personuppgiftsincidenter, integritetspolicyn och PUL-policyn. Uppdateringarna har framför allt skett utifrån nya kamerabevakningslagen.

Innehållet i styrdokumenten bedöms hålla god kvalitet vad gäller relevant information och enkelt språk. Vidare bedöms arbetet med uppdateringar och översyn av styrdokumentationen som god, vilket innebär att arbetet med kvaliteten av innehållet är under ständig förbättring.

Bristerna som har identifierats i dokumentationen bedöms inte vara av allvarliga slag.

Likt förra året konstaterar DSO att de brister som iakttagits gällande dataskydd inte ligger i avsaknad av dokumentation, utan snarare i brist på förståelse och kunskap ute i verksamheten. Styrdokument, oavsett relevans eller kvalitet, är oftast inte till någon större hjälp ute i verksamheten om kunskapen inom området är låg. Andra insatser, såsom utbildning och muntlig information, kan ha större relevans för att öka medvetenheten och därmed möjligheten till ett systematiskt dataskyddsarbete. Med det sagt är styrdokument viktiga verktyg för bland annat de roller som arbetar mer frekvent med frågorna samt för att kunna visa regelefterlevnad vid tillsyn. Att arkivarien under året har utbildat verksamheten kring styrdokument är ur denna synpunkt positivt.

Organisatoriska säkerhetsåtgärder har under året förbättrats i och med att arkivarien har gått utbildat och gått igenom anvisningar till verksamheten.

I hanteringsanvisningen sker en hänvisning till registerförteckningen för att sammankoppla hanteringsanvisning gällande information med var det finns personuppgifter. Det sker en avstämning mellan dataskyddssamordnare och arkivarie så att hänvisningarna blir korrekta. Hanteringsanvisningarna är också kopplade till gallringsanvisningarna.

Informationsklassning

Under 2023 genomfördes ett projekt för att se över systematiken gällande hur informationsklassningen sker och verksamheten beslutade att fortsätta enligt nuvarande systematik. Det innebär att informationsklassningen även fortsatt kommer att ske med utgångspunkt från system i stället för informationsmängd och/eller process. Ingen ändring har skett i detta beslut för 2025.

Informationsklassning har genomförts för samtliga 18 system som används av verksamheten. Under året har signeringsverktyg bytts ut och i samband med det uppdaterades den tidigare informationsklassningen. Swedbank Pay har också klassats, även om de är en underleverantör, för att ha kontroll över hela leveranskedjan.

Det finns vissa personuppgiftsbehandlingar som inte sker i ett system, utan som finns i kartotek. Dessa är inte informationsklassade men de finns med i registerförteckningen.

Informationssäkerhetssamordnaren har en systemdokumentation där det framgår vilka bedömningar som har gjorts gällande behovet av informationsklassning samt på vilken nivå systemet har klassificerats. I dokumentationen framgår vidare om personuppgifter behandlas i systemet eller inte.

Bristerna som har noterats är samma som förra året, det vill säga att klassning sker utifrån system i stället för processer. KHST har dock gjort ett aktivt val att behålla klassningen enligt nuvarande system och är medveten om att det kan medföra vissa risker, men dessa bedöms som små. Med hänsyn till att registerförteckningen får anses vara tämligen komplett och därmed ge personuppgiftsansvarige en bra överblick gällande personuppgiftsbehandlingarna och de system som används tillsammans med att samtliga system är klassade bedöms risken inte vara av allvarligt slag.

KHST arbete med informationsklassningar framstår som väl fungerande och informationssäkerhetssamordaren har nödvändig dokumentation över de system där personuppgiftsbehandlingar sker. Även om vissa brister har identifierats vad gäller framför allt metoden att klassa system i stället för informationsmängder framkommer inga brister av sådant slag att det föranleder DSO att rekommendera några omedelbara ändringar men däremot är det viktigt att KHST är medveten om de risker som tas upp i detta avsnitt.

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, ändamålsenliga rutiner och styrdokument finns på plats.

Rekommendationen är att fortsätta det systematiska arbetet med styrdokument.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

I och med den nya mallen genomförs tröskelanalyser.

Rekommendationen är att fortsätta det systematiska arbetet med styrdokument.

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

Mall och rutiner finns.

Rekommendationen är att fortsätta det systematiska arbetet med styrdokument.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

Konsekvensbedömningar genomförs men bedömningen och rekommendationen sedan tidigare är att de innehållsmässigt inte håller tillräcklig kvalité. Dock är bedömningen att detta kan komma att förbättras i och med den nya mallen.

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

I stor utsträckning är bedömningen att de behandlingar som kräver en konsekvensbedömning är identifierade men rekommendationen är fortsatt att göra en tröskelanalys gällande biblioteksverksamheten.

Dataskyddsombudets jämförelse med föregående års resultat

Resultatet är i stor utsträckning densamma som förra året på så vis att KHST arbetar systematiskt med frågorna och ständiga förbättringar sker (även om det är fortsatt personbundet).

Dataskyddsombudets bedömning samt rekommendationer

Av vad DSO kan bedöma så är de behandlingar som kräver en konsekvensbedömning identifierade. Konsekvensbedömningarna gås igenom i samband med den årliga revisionen av registerförteckningen och på så vis säkerställs att de är aktuella. Under förra året har kamerabevakningen utökats på så vis att kamerabevakning av offentliga utrymmen sker. Konsekvensbedömning för detta har skett under 2025.

DSO anser dock att kvaliteten på konsekvensbedömningarna som DSO tagit del av inte håller en tillräckligt hög kvalitet i alla delar. Konsekvensbedömningarna skulle därför behöva ses över för att säkerställa tillräcklig kvalitet även om en förbättring skett i och med att de lades in i Draftit.

DSO har under arbetet med årsrapporten från 2023 lyft frågan gällande behovet av konsekvensbedömning inom biblioteksverksamheten. Dataskyddssamordnaren uppgav då att verksamheten inte har tagit ställning till om det behövs någon sådan. Av den information som DSO fått vid upprättande av 2025 års rapport så har Stockholm stad gjort bedömningen att någon konsekvensbedömning av bibliotekssystemet inte är nödvändigt. DSO konstaterade att i granskningen av bibliotekssystemet som skedde under 2025 så framkom det av informationsklassningen av systemet att stora mängder personuppgifter behandlas och att det behandlas känsliga personuppgifter. Personuppgifterna delas mellan alla bibliotek och det finns integrationer mot många andra system. Det finns med andra ord många omständigheter som talar för att en konsekvensbedömning behöver göras.

DSO bedömer det som positivt att verksamheten väljer att ta fram nya konsekvensbedömningar som är mer omfattande och anser att kvaliteten på innehållet i konsekvensbedömningarna kommer att öka i samband med detta.

DSO rekommenderar att verksamheten gör en riskbedömning gällande biblioteksverksamheten för att bedöma om en konsekvensbedömning behöver genomföras. Detta med hänsyn till att det mest troligt förekommer en stor mängd personuppgifter inom biblioteksverksamheten, däribland barns personuppgifter.

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?

Majoriteten av begäran hanteras av kundtjänst löpande. Det förs ingen statistik så frågan kan inte besvaras.

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

Majoriteten av begäran hanteras av kundtjänst löpande. Det förs ingen statistik så frågan kan inte besvaras.

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

Majoriteten av begäran hanteras av kundtjänst löpande. Det förs ingen statistik så frågan kan inte besvaras.

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

Majoriteten av begäran hanteras av kundtjänst löpande. Det förs ingen statistik så frågan kan inte besvaras.

Dataskyddsombudets jämförelse med föregående års resultat

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

Resultatet är i stor utsträckning densamma som förra året.

Dataskyddsombudets bedömning samt rekommendationer

Under 2025 har det kommit inte kommit några begäran om registerutdrag.

Vad gäller begäran om rättelse och radering är det något som kommer in löpande till kundtjänst och är främst kopplat till biljettsystemet och biblioteket. Det förs ingen separat statistik över begäran kopplade till dataskyddsförordningen, utan alla frågor och begäran av alla slag hanteras av kundtjänst i den dagliga verksamheten.

Bedömningen från dataskyddssamordnaren är att samtliga löpande begäran till kundtjänst hanteras inom rätt tid och att hanteringen följer den rutin som framgår av integritetspolicyn.

Vad gäller registerutdrag hanteras de av dataskyddssamordnaren. Registerutdragen hanteras manuellt och väl inom tidsfristen tidigare år.

Med hänsyn till att det inte finns någon statistik eller annat underlag över hur många begäran rörande registrerades rättigheter som kommer in utöver begäran om registerutdrag går det inte att bedöma hur dessa begäran hanteras utöver registerutdrag.

Vad gäller registerutdrag kan konstateras att de hanteras manuellt, vilket kan utgöra en risk. Med hänsyn till att det för nuvarande är en väldigt låg förfrågan om att få ut registerutdrag bedöms risken inte som överhängande.

Även i år rekommenderar DSO att verksamheten gör stickprovskontroller gällande begäran från registrerade för att få en uppfattning om omfattningen av begäran enligt dataskyddsförordningen och om någon utbildning eller rutiner krävs för kundtjänst utifrån resultatet av kontrollen. Vid den granskning som DSO gjorde förra året av kundtjänst framgick att det fanns en osäkerhet bland medarbetarna om bestämmelser om sekretess och dataskydd, vilket bör följas upp.

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?

Utöver styrdokument och information på intranätet genomför dataskyddsamordnaren riktade utbildningar.

Rekommendationen är att de riktade utbildningarna bör fortsätta eftersom bedömningen är att det finns risk för att inte alla incidenter anmäls med hänsyn till det låga antalet anmälda personuppgiftsincidenter.

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

Styrdokument och rutiner finns och bedöms följas när dataskyddssamordnare och informationssäkerhetssamordnare får information om eventuell incident.

Risken som identifierats är att verksamheten på grund av kunskapsbrist möjligen inte rapporterar in alla eventuella incidenter och därmed följs inte rutinerna.

Hur många personuppgiftsincidenter har dokumenterats under året?

Fyra stycken.

Hur många personuppgiftsincidenter har anmälts till IMY under året?

Ingen av de inrapporterade incidenterna har ansetts vara så allvarliga att de behöver anmälas till IMY.

Dataskyddsombudets jämförelse med föregående års resultat

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

Resultatet är i stor utsträckning densamma som förra året på så vis att KHST arbetar systematiskt med frågorna och ständiga förbättringar sker (även om det är fortsatt personbundet).

Dataskyddsombudets bedömning samt rekommendationer

Med hänsyn till det väldigt låga antalet internt anmälda incidenter finns det inte tillräckligt med underlag för att dra några säkra slutsatser.

Det som kan konstateras är att antalet internt anmälda personuppgiftsincidenter är fortsatt låg, vilket i sig kan indikera att kunskapen i verksamheten kring vad som är en personuppgiftsincident är bristfällig och därmed anmäls inte sådant som borde anmälas. Det får därför antas att det finns ett mörkertal gällande inträffade personuppgiftsincidenter. Det bör understrykas att ca 100 säkerhetsincidenter rapporteras in varje år och att de i stor utsträckning rör arbetsmiljö eller borttappade elektronik.

Dataskyddssamordnaren och informationssäkerhetssamordnaren är av uppfattningen att det mest troligt finns personuppgiftsincidenter som inte rapporteras in men att dessa mest troligt inte är av någon allvarligare slag. Det rör sig framför allt felskickade mejl men där verksamheten har slutat att anmäla dessa eftersom uppfattningen är att dessa ändå så inte bedöms vara av allvarligt slag som leder till rapportering till IMY. Dessa felskick rör framför allt interna felskick till personer med samma eller liknande namn.

Det som talar för att incidenterna inte är av allvarligare slag är att en stor del av kärnverksamheten inte hanterar personuppgifter i någon större omfattning. För den administrativa personalen, där det får antas att risken för personuppgiftsincidenter är som störst, håller dataskyddssamordnaren riktade utbildningar med jämna intervall. Det finns dessutom riktlinjer och rutiner gällande hur en personuppgiftsincident ska hanteras.

DSO:s uppfattning är densamma som förra året, det vill säga att personuppgifterna hanteras på ett acceptabelt sätt även om det finns viss kunskapsbrist bland personalen vad en personuppgiftsincident är. Överlag är dock uppfattningen att personuppgifter hanteras i de system de är avsedda att behandlas i och att några större risker inte identifierades. Det finns dock anledning att göra stickprovskontroller inom de områden där risken för personuppgiftsincidenter är högst, såsom HR och kundtjänst.

Rekommendationen är särskilda insatser sätts in för att komma till rätta men den låga frekvensen av inrapporterade personuppgiftsincidenter. Ett råd är att göra stickprovskontroller inom områden där det hanteras större mängd personuppgifter för att kontrollera eventuella incidenter.

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.[2]

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?

Några kontroller har inte genomförts av DSO kring detta inför 2025 och frågan kan därför inte besvaras med säkerhet. DSO har endast gjort en förfrågan och fått information om att det finns rutiner på plats vid upphandling och inköp av system för att identifiera personuppgiftsbehandlingar och eventuella överföringar.

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?

Det finns rutiner för att bedöma vad för slags överföringsverktyg som krävs vid överföring.

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

I de fall det har bedömts att en TIA krävs har detta genomförts enligt information från informationssäkerhetssamordnaren.

Dataskyddsombudets jämförelse med föregående års resultat

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

[2] 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.

Detta granskningsområde är nytt för år 2025 och det finns därför inga resultat att jämföra med från tidigare år.

Dataskyddsombudets bedömning samt rekommendationer

Tredjelandsöverföringar har inte granskats särskilt och rekommendationen är att detta område granskas under 2026.

Bilaga 2 – Andra genomförda granskningar och omvärldsbevakning

Andra granskningar som dataskyddsombudet har genomfört under året

Genomförda granskningar:

- Granskning av biblioteksystemet
- Granskning av e-Dok

Granskning 1 Biblioteksystemet

Slutsatsen från granskningen var att KHST bör utreda frågorna kring personuppgiftsansvar för att klargöra om det föreligger gemensamt personuppgiftsansvar eller någon biträdessituation mellan KHST och kulturförvaltningen. Med hänsyn till den stora mängd personuppgifter som hanteras är det viktigt att frågor kring registrerades rättigheter och incidenthantering är utredda och att det finns tydliga rutiner för att hanteras dem. I denna del vill DSO även framföra att biblioteksystemet kommer att ha många olika integrationer och KHST bör säkerställa om dessa integrationer innebär att låntagarnas personuppgifter kommer att delas mellan flera olika leverantören. Framför allt gäller detta integrationen mot ekonomisystemet där det bör utredas om det sker realtidssynkronisering eller om uppgifter hämtas vid behov. Det är även viktigt att frågan om leverantören av biblioteksystemets status gentemot KHST utreds så att frågan om äganderätt till data med mera är säkerställd. Slutligen anser DSO att KHST tillsammans med kulturförvaltningen bör kontrollera frågan kring hanteringen av känsliga personuppgifter med hänsyn till att informationsklassningen och utkastet till personuppgiftsbiträdesavtal säger olika saker för att säkerställa att säkerhetsåtgärderna som införs är på lämplig nivå.

KHST har tagit upp frågan med Stockholm stad efter DSO:s granskning men inga åtgärder har vidtagits från staden.

Granskning 2 e-Dok

Slutsatsen från granskningen var att eDok är ett gemensamt system som samtliga förvaltningar och bolag inom Stockholms stad använder. Systemet har en central förvaltning men varje enhet inom staden ansvarar för sin egen diarieföring och använder systemet på olika sätt.

DSO anser att KHST bör utreda frågorna kring personuppgiftsansvar för att klargöra ansvaret mellan KHST och kommunstyrelsen. Med hänsyn till att varje användarorganisation har möjlighet att upprätta instruktioner utgår DSO från att en bedömning har gjorts att det är kommunstyrelsen är personuppgiftsbiträde åt övriga nämnder och bolag. Av den information DSO fått finns ingen instruktion mellan KHST och kommunstyrelsen, vilket borde finnas på plats enligt DSO:s bedömning.

Beroende på vad som har utretts sedan tidigare bör även frågan om det föreligger ett personbiträdesförhållande mellan varje enskild användarorganisation och TietoEvry i någon utsträckning också klarläggas.

Efter DSO:s granskning har KHST tagit upp frågan med Stockholm stad och initierat ett arbete med att skriva instruktioner. KHST har även påpekat vissa brister gällande ansvarsfördelningen.

Dataskyddsombudets rekommendationer
Rekommendation från DSO gällande bibliotekssystemet var 1. Utred personuppgiftsansvaret inom det gemensamma bibliotekssystemet 2. Beroende på vad första punkten visar överväg nödvändigheten av en överenskommelse kring gemensamt personuppgiftsansvar och/eller personuppgiftsbiträdesavtal Rekommendationen från DSO gällande e-Dok var 1. Utred personuppgiftsansvaret 2. Beroende på vad första punkten visar överväg nödvändigheten av en överenskommelse kring gemensamt personuppgiftsansvar och/eller personuppgiftsbiträdesavtal/reglemente/instruktioner

Övrigt att rapportera

Utifrån årets granskningar, men även med hänsyn till förra årets granskningar, är DSO:s rekommendation att det fortsatta arbetet fokuserar på de områden där risken för de registrerades rättigheter är som störst. Det innebär att arbetet bör fokusera på personuppgiftsincidenter, konsekvensbedömningar och behandlingen av känsliga och integritetskänsliga personuppgifter.

DSO kan konstatera att det finns en vilja och fokus på dataskyddsarbetet hos KHST och att området har prioritet och utvecklas och förbättras, bland annat utifrån de råd och rekommendationer som lämnas av DSO. Detta är mycket positivt. Kunskapen och kompetensen hos nyckelpersonerna är god och dessa nyckelpersoners insatser är också det som till stor del driver arbetet framåt. Andra sidan av detta mynt är att personberoendet är stort, vilket i sig är en risk.

KHST bör fastställa en dataskyddsorganisation med tydligt utpekade ansvarsroller även för personer i verksamheten. Det rekommenderas att en eller flera personer inom de verksamhetsområden där det behandlas personuppgifter i stor omfattning och /eller känsliga personuppgifter hanteras får en utpekad roll med ansvar för dataskyddsfrågor