Stockholms stad

Bilaga 10

GDPR Årsrapport

År 2024

Kulturhuset Stadsteatern AB

GDPR årsrapport
Januari 2025

Dnr: 2025/4
Utgivningsdatum: 20250108
Kontaktperson: Petra Kanon, IT-Säkerhetsbolaget i Skandinavien AB

1 Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

Enligt dataskyddsförordningen är varje nämnd och bolagsstyrelse inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnd och bolagsstyrelse behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett Dataskyddsombud (”DSO”). DSO:s har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är således ett medel för nämnd och styrelse att ta emot de råd och rekommendationer som DSO:s är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:s granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnd eller bolagsstyrelse ska kunna *visa* att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna *dokumenteringsskyldighe*t. Årsrapporten är även ett medel för nämnds/bolagsstyrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehåll

2 Sammanfattning

I egenskap av Dataskyddsombud lämnar jag följande årsrapport.

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 och hantering av personuppgifter i e-post bland annat.

Den samlade risknivån bedöms som acceptabel och riksnivån bedöms också ha minskat jämfört med förra året med hänsyn till de förbättringar som skett.

3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som Personuppgiftsansvarig (”PUA”) som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som dataskyddsförordningen avser.

De obligatoriska rapporteringsområdena är registerförteckning, styrdokument, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, konsekvensbedömningar, individens rättigheter och personuppgiftsincidenter.

Nedan redogörs för verksamhetens status och DSO:s slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:s genomförda uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	76
Har nödvändiga uppdateringar gjorts?	Ja
Bedöms registerförteckningen vara fullständig?	Ja
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

Det är ett krav enligt dataskyddsförordningen att den personuppgiftsansvarige för ett register över de behandlingar som utförs under dess ansvar.

En fullständig och uppdaterad registerförteckning skapar en intern synlighet och förståelse för vilka personuppgifter som behandlas

samt hur de hanteras. Registerförteckningen är därför dataskyddsarbetets centrala utgångspunkt och säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling samt att personuppgifterna behandlas för de ändamål de har samlats in för. På så vis säkerställs även den registrerades fri- och rättigheter på ett systematiskt sätt.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

Det finns 76 behandlingar registrerade i Draftit, vilket är två fler än förra året.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Uppdateringar sker systematiskt en gång per år samt löpande vid behov. Vid kontroll i Draftit har uppdateringar skett under september till november 2024.

DSO bedömer hur fullständig registerförteckningen är

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.

Vid intervju med dataskyddssamordnaren förra året uppgavs att i och med den systematiska uppdateringen en gång per år förbättras innehållet i varje behandling kontinuerligt, vilket innebär att även innehållet blir mer komplett.

DSO har vid fråga till dataskyddssamordnaren om var kontaktuppgifter till dataskyddsombudet finns fått svaret att det ligger samlat på ett ställe i Draftit med angivet namn och telefonnummer. Förra året ansågs DSO att det var en brist att kontaktuppgifter inte fanns med, vilket i år är klarlagt att det finns.

Likt förra årets rapport noterar dataskyddsombudet att vissa behandlingar bör kontrolleras gällande rättsliga grunden *avtal* som

bedöms användas för behandlingar där den grunden inte är tillämplig.[1]

DSO har noterat att samtycke används som rättslig grund i anställningsförhållanden. Problemet med detta är att samtycke kräver ett jämlikt maktförhållande, vilket inte sker mellan en arbetsgivare och arbetstagare. Samtycke är således ingen lämplig rättslig grund i anställningsförhållanden.

DSO har uppmärksammat att det saknas en kolumn för extra skyddsvärda (integritetskänsliga) personuppgifter. Trots att det inte är ett krav enligt GDPR skulle en kolumn underlätta arbetet med att identifiera och kunna vidta lämpliga säkerhetsåtgärder för den kategorin uppgifter. DSO har även noterats en avsaknad av en kolumn för rättslig grund för tredjelandsöverföring. Detta noterades även i granskningen av registerförteckningar från 2023. Inte heller denna är en obligatorisk uppgift men det underlättar dataskyddsarbetet om denna information finns med.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Som stöd för att registrera personuppgiftsbehandlingar finns *Vägledning – Inventering av personuppgifter* från Stockholm stad samt en hanteringsanvisning. Utöver det finns det information om DraftIt på intranätet. 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.

Vidare håller dataskyddsamordnaren utbildning för framför allt administrativ personal som är de som främst hanterar personuppgifter inom verksamheten. Dataskyddsamordnaren har också kontakt med de ansvariga för behandlingarna och påminner om att kontrollera att behandlingarna är aktuella och korrekta, vilket har höjt medvetenheten bland kärnverksamheten gällande att anmäla och uppdatera personuppgiftsbehandlingar.

Bedömningen är att det finns lämpliga rutiner och strukturer på plats men att utmaningen är att se till att de tillämpas ute i

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

verksamheten. Utvecklingen i den delen verkar dock gå framåt, vilket är positivt.

Risken som DSO kan notera 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 som upprätthåller arbetet.

3.1.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

De identifierade bristerna som är värd att nämna är rättsliga grunder rörande anställningsförhållande och de fem utvalda behandlingar som har avtal som rättslig grund. 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.

3.1.5 DSO ger råd och rekommendationer till PUA

Personuppgiftsansvarige bör fokusera på att öka kvaliteten av innehållet i registerförteckningen. Rättsliga grunden bör ses över för de behandlingar som använder samtycke i anställningsförhållanden samt de fem behandlingar som använder avtal.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Ja
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Ja
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Ja
Är dokumenten uppdaterade?	Ja
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja

3.2.2 Syfte

Genom styrdokument kan den personuppgiftsansvarige både visa att ett systematiskt dataskyddsarbete bedrivs och hur verksamheten ska hantera personuppgifter.

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?

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 personuppgifter i e-post har dataskyddsombudet i år fått del av ”Rutin för hantering av personuppgifter i e-posten” som ger vägledning för hur personuppgifter ska hanteras. Det nämns bland annat att

personuppgifter ska undvikas i e-post och framför allt känsliga personuppgifter. Detta är mycket positivt.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

Innehållet 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. Det som kan behövas är en översyn för att samla viss information i samma dokument.

3.2.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
x	Inga brister av nämnvärd betydelse identifierade

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

3.2.5 DSO ger råd och rekommendationer till PUA

Det finns en stor mängd styrdokument och en rekommendation är att se över om det går att samla viss information i färre dokument.

Vad gäller internt inrapporterade personuppgiftsincidenter kan konstateras att problemet kring incidentrapportering mest troligt inte ligger i avsaknad av dokumentation, utan snarare i brist på förståelse och kunskap ute i verksamheten. Verksamheten bör därför fortsätta med de riktade utbildningsinsatserna för att öka medvetenheten hos de anställda gällande personuppgiftsincidenter. Detta påpekande får även antas ha generell räckvidd. 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.

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

3.3.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	Samtliga 16 system är klassade
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 Syfte

Dataskyddsförordningen ställer krav på att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifter. Precis som registerförteckningen utgör en informationsklassning en bas för att kunna arbeta systematiskt med dataskydd och för att kunna identifiera risker och nödvändiga säkerhetsåtgärder.

3.3.3 Resultat

Under förra året har det genomförts 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 2024.

Undre året har informationssäkerhetssamordnaren påbörjat informationsklassning av lönekartläggningssystemet AON och under hösten 2024 fokus varit på kontinuerliga sårbarhetstester. KHST har vidare bedömt att de inte omfattas av NIS2.

Informationssäkerhetssamordnaren anser att medvetenheten bland organisationen har ökat gällande att olika informationsmängder behöver hanteras på olika sätt.

Organisatoriska säkerhetsåtgärder har under året förbättrats i och med att en arkivarie har anställts. Arkivarien har under året arbetat mycket med vad för information som ska lagras och var det ska

lagras samt frågan om gallring. Arkivarien har vidare under året implementerat utifrån hanteringsanvisningarna (som är del av dokumenthanteringsplanen för staden) och kontrollerat att de följs samt haft en utbildning kring frågorna för 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.

Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?

Informationsklassning har genomförts för samtliga 16 system som används av verksamheten. Inga nya system har tagits in under 2024 som har varit i behov av informationsklassning. Ett system har fasats ut sedan förra året. En översyn har gjorts av HR-systemet vilket har lett till beslutet att ett av dessa ska informationsklassas och detta pågår.

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.

Är klassade personuppgiftsbehandlingar aktuella?

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.

Klassningarna har fått en översyn under 2023 i samband med det projekt som genomfördes och nödvändiga uppdateringar har gjorts i form av att ett system som inte längre används har plockats bort och informationsklassning har skett av det nya systemet.

3.3.4 Hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
x	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

Informationsklassning har genomförts för samtliga system.

Bristerna som har noterats, och som även KHST är medvetna om, är att det kvarstår information som ännu inte klassificerats i kartotek. Ur dataskyddshänseende bedömer DSO emellertid inte detta som någon risk av nämnvärd betydelse för de registrerades fri- och rättigheter eftersom behandlingarna finns med i registerförteckningen och det har vidtagits lämpliga säkerhetsåtgärder kring kartoteken. Dataskyddssamordnaren har även informerat om vikten att inge ange fler personuppgifter än nödvändigt i korten samt att känsliga personuppgifter inte får förekomma.

Utifrån vad som sagts ovan är det rimligt att anta att lämpliga tekniska och organisatoriska åtgärder är vidtagna för systemen. Notera dock att granskningen inte omfattat stickprovskontroller för att verifiera detta i vidare bemärkelse, utan granskningen har endast bestått av en intervjuer med relevanta funktioner.

Det brist som DSO noterat är att informationsklassningen utgår från system i stället för behandlingar eller processer. Det kan inte uteslutas att det kan innebära en risk vad gäller förbiseende av vad för slags personuppgifter som faktiskt behandlas inom systemen och hur olika enskilda informationsmängder tillsammans kan få ett större skyddsvärde än vad som kan vara fallet om man endast klassar system.

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.

3.3.5 DSO ger råd och rekommendationer till PUA

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.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Ja
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Ja
Är de genomförda bedömningarna aktuella?	Ja

3.4.2 Syfte

Konsekvensbedömningen hjälper en organisation att identifiera och minimera integritetsriskerna för personuppgifter som behandlas. En konsekvensbedömning har till syfte att identifiera och dokumentera risker kopplade till en viss behandling samt att bedöma sannolikheten och konsekvensen om riskscenariot skulle inträffa.

3.4.3 Resultat

Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?

Dataskyddssamordnaren har en lista över de behandlingar där konsekvensbedömningar har genomförts. Det har genomförts 15 konsekvensbedömningar för verksamheten.

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. DSO har noterat att det fortfarande inte har fattats något beslut kring biblioteksverksamheten. Det kan finnas ett behov av en konsekvensbedömning för den verksamheten eftersom barns personuppgifter behandlas.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Under 2024 har inga nya konsekvensbedömningar gjorts. Under året har kamerabevakningen utökats på så vis att kamerabevakning av offentliga utrymmen sker. Konsekvensbedömning för detta kommer att ske under 2025.

DSO konstaterar att det kan finnas anledning att kontrollera behandlingarna inom biblioteksverksamheten för att bedöma om någon konsekvensbedömning behövs inom denna del.

Är de genomförda konsekvensbedömningarna aktuella?

Konsekvensbedömningarna bedöms vara aktuella. Konsekvensbedömningarna gås igenom i samband med den årliga revisionen av registerförteckningen och på så vis säkerställs att de är aktuella. I år har uppdateringar gjort genom att genomförda konsekvensbedömningar förts in i Draftit och i samband med det kompletterades konsekvensbedömningarna med uppgifter som var allmänt kända eller som gick att hämta från registerförteckningen. På så vis är konsekvensbedömningarna numera något mer fullständiga. I samband med detta har också personuppgiftsansvarige beslutat att gå över till den mall för konsekvensbedömningar som finns i Draftit.

DSO har även i samband med upprättandet av årsrapporten kontrollerat att behandlingarna i konsekvensbedömningen stämmer överens med hur de upprättats i registerförteckningen. Samtliga behandlingar som konsekvensbedömts finns även i registerförteckningen.

DSO anser dock att kvaliteten på konsekvensbedömningarna som DSO tagit del av inte håller en tillräckligt hög kvalitet. Detta eftersom de är för kortfattade samt har undermåliga hänvisningar till andra dokument. 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.

3.4.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
x	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

DSO har vid bedömningen tagit hänsyn till kvaliteten och innehållet i de faktiska konsekvensbedömningarna. Vid granskning av konsekvensbedömningarna ansåg DSO att dessa har ett tunt innehåll. Dessutom saknas det hänvisningar till andra dokument. Det innebär att dessa blir svåra att följa.

Under året har beslut fattats att ta fram en ny mall för konsekvensbedömningar. DSO:s bedömning är att i och med att den nya mallen kommer framtida konsekvensbedömningar att hålla ett mycket högre kvalitet och uppfylla lagkraven.

DSO har vid bedömningen även tagit hänsyn till att det kan finnas ett behov av en konsekvensbedömning för biblioteksverksamheten samt kamerabevakning. Trots förbättringar som skett med att införa och uppdatera konsekvensbedömningarna i Draftit så blir bedömningen att risken har ökat i år i och med att det i år finns två eventuella högriskbehandlingar inte har konsekvensbedömts.

3.4.5 DSO ger råd och rekommendationer till PUA

DSO bedömer det som positivt att verksamheten väljer att ta fram nya konsekvensbedömningar som är mer omfattande. DSO bedömer 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.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	0 registerutdrag Löpande begäran av radering eller rättelse av konton (samma förra året). Går att logga in själv och ändra men kan även ringa kundtjänst
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	Okänt.

3.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen ett antal rättigheter som på olika sätt ska garantera att den registrerade personen har insyn i hur dennes personuppgifter hanteras samt har en viss kontroll över personuppgiftsbehandlingen. Det är ett krav enligt förordningen att den verksamhet som enligt förordningen är att se som personuppgiftsansvarig tillgodoser rättigheterna i fråga inom trettio dagar efter att ha mottagit begäran.

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

Under 2024 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.

3.5.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
x	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

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.

3.5.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar 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.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Riktade utbildningar och information på intranätet
Hur många personuppgiftsincidenter har dokumenterats?	Av de ca 100 inrapporterade incidenterna har ingen klassats som personuppgiftsincident
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	0
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	N/A

3.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskyddsförordningen 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.

En personuppgiftsincident kan få allvarliga konsekvenser för en enskild och det är därför viktigt att det finns rutiner för att upptäcka, hantera och förhindra incidenter i en verksamhet.

3.6.3 Resultat

Hur väl förmår verksamheten att rapportera personuppgiftsincidenter i tid till Integritetsskyddsmyndigheten?

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

3.6.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
x	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

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 ända 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 och i år har särskild insats gjorts gällande personuppgiftsincidenter. Det finns dessutom riktlinjer och rutiner gällande hur en personuppgiftsincident ska hanteras. DSO har under året utfört granskningar mot HR och kundtjänst där stora mängder personuppgifter och även stora mängder känsliga personuppgifter (inom främst HR) behandlas för att få en uppfattning om hur

personuppgifter hanteras inom dessa områden. Med hänsyn till KHST:s verksamhet är det troligt att en stor del av potentiella personuppgiftsincidenter sker inom dessa två områden. Efter granskningarna är DSO:s uppfattning 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.

Att personuppgiftsincidenter inte upptäcks är mycket allvarligt och kan innebära höga risker för de registrerade. Med anledning av det mest troligt föreligger ett mörkertal innebär det en risk eftersom verksamheten inte har kontroll över denna fråga. Med hänsyn till den insyn i verksamheten som DSO har vid tiden för denna rapport är dock bedömningen, till skillnad från förra året, att risken är något lägre. Detta grundar sig framför allt på de granskningar som genomförts av HR och kundtjänst.

3.6.5 DSO ger råd och rekommendationer till PUA

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.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- HR-processerna
- Hantering av personuppgifter i biljetter och e-post hos kundtjänst
- Extern kommunikation

4.2 Syfte

En central del av arbetet för ett dataskyddsombud är att göra återkommande granskningar av hur väl dataskyddsförordningen efterlevs. Resultaten av granskningarna påverkar i stor utsträckning vilka beslut verksamheten kan fatta i fråga om dataskyddsåtgärder. För PUA är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under det gångna året och vad resultaten av granskningarna är.

4.3 Genomförda granskningar och deras resultat

HR-processerna

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
x	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

Slutsatsen från granskningen av HR-processerna var att de anställda är medvetna om att anställdas personuppgifter är av känslig natur och att uppgifterna ska hanteras utifrån det. Däremot identifierades

brister i hanteringen av medarbetarsamtal, personalärenden och sjukintyg.

Rekommendation från DSO var att ta fram rutiner kring hanteringen av medarbetarsamtal, personalärenden och sjukintyg. DSO rekommenderade även KHST att utreda om det fanns risk att personuppgifter överförs till tredje land vid användning av systemen från Talentech och om så är fallet, säkerställa att överföringen är i enlighet med kraven i dataskyddsförordningen. Vidare rekommenderade DSO att utreda frågan kring att HR skulle ta fram mer statistik än tidigare och om behandlingen i sådana fall är laglig.

Hantering av personuppgifter i biljetter och e-post hos kundtjänst

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
x	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

Slutsatsen från granskningen gällande personuppgiftshantering i e-post och biljetter var att medarbetare inom kundtjänst inte känner till några e-postrutiner. Vidare anser sig medarbetare ha dålig koll på GDPR och de hinner inte titta på förinspelade utbildningsvideor.

Rekommendationen från DSO var att inför enklare e-postrutiner för att öka medvetenheten bland anställda. Vidare föreslogs att KHST avsätter tid för att medarbetare ska hinna titta på utbildningsvideor om GDPR för att kunna öka kunskapen.

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
x	Inga brister av nämnvärd betydelse identifierade

Slutsatsen från granskningen är att KHST har väl utarbetade styrdokument samt rutiner med bland annat samtycke gällande publicering av barns personuppgifter i sociala medier och att dessa rutiner också följs i praktiken. Bedömningar kring användningen av sociala medier har genomförts för några år sedan.

Bedömningen är att risken bedöms som låg och att inga brister har identifierats i hanteringen.

4.4 DSO ger råd och rekommendationer till PUA

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.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- Systematiskt dataskyddsarbete inom hela verksamheten
- Personuppgiftsincidenter
- Konsekvensbedömningar

5.2 Syfte

Syftet är att lyfta fram övergripande risker inom dataskydd.

5.3 Resultatet av riskkartläggningen

Systematiskt dataskyddsarbete inom hela verksamheten

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
x	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

Likt förra året konstaterar DSO att det systematiska dataskyddsarbetet inte är utvecklat inom KHST, utan dataskyddsarbetet är mycket personberoende. DSO ser dock tendenser att medvetenheten ökar något inom organisationen även om det iakttagits brister i kunskapen på granskade områden. Under året har en arkivarie anställts som bedöms kunna minska personberoendet. 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.

Utifrån vad som sagts döms risken som lägre i år än förra året.

5.4 DSO ger råd och rekommendationer till PUA

KHST bör fastställa en dataskyddsorganisation med tydligt utpekade ansvarsroller. 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.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Biblioteksverksamheten
- Marknadsavdelningen
- Administrativa avdelningen

6.2 Syfte

En av dataskyddsombudets viktigaste uppgifter är att granska efterlevnaden av dataskyddsförordningen. Detta görs lämpligast genom riktade granskningar under året.

6.3 Planerade granskningar

Biblioteksverksamhet

Inom biblioteksverksamheten behandlas en stor mängd personuppgifter inom låneverksamheten. En stor del av dessa uppgifter bedöms vara barn. Det finns därför anledning att kontrollera denna verksamhet för att identifiera risker.

Marknadsavdelningen

Inom marknadsavdelningen hanteras stora mängder personuppgifter och med hänsyn till den spridning som information kan få via marknadsavdelningen kan det föreligga höga risker gällande integritetsskydd varför det finns anledning att kontrollera denna verksamhet närmare.

Administrativa avdelningen

Inom administrativa avdelningen hanteras stora mängder personuppgifter och det kan därmed föreligga höga risker gällande integritetsskydd varför det finns anledning att kontrollera denna verksamhet närmare,