GDPR Årsrapport

År 2023

Kulturhuset Stadsteatern AB

GDPR årsrapport
Januari 2023

Dnr:
Utgivningsdatum: 2023-01-11
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 ert 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 låg, vilket mest troligt förklarar den låga frekvensen av inrapporterade personuppgiftsincidenter.

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?	74
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 74 behandlingar registrerade i Draftit, jämfört med 72 stycken förra året.

Något som är värt att notera är att endast 8 behandlingar är godkända medan övriga behandlingar har statusen ”under behandling”. Dataskyddssamordaren har efter förfrågan från DSO uppgett att det handlar om ett förbiseende och att samtliga inlagda behandlingar i realiteten är godkända. Vidare kan noteras att risknivå har angetts för endast 3 behandlingar. Dataskyddssamordnaren har efter förfrågan från DSO uppgett att detta inte är uppdaterat i Draftit.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Vid kontroll i Draftit framgick att de flesta behandlingar har ändrats under september 2023 i samband med att dataskyddsamordnaren uppdaterade behandlingarna med information kring gallringsfrister.

Vid intervju med dataskyddssamordnaren har det uppgetts att uppdateringar sker systematiskt en gång per år samt löpande vid behov. De behandlingar som inte fanns med i registerförteckningen vid förra årets granskning har nu förts in och vissa behandlingar inom HR har justerats.

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 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.

Vid stickkontroll av fem slumpvis utvalda behandlingar i Draftit instämmer DSO att innehållet håller en godtagbar nivå men att en kontroll bör göras gällande rättsliga grunden *avtal* som bedöms användas för behandlingar där den grunden inte är tillämplig.[1]

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

Risken som DSO kan notera är att upprätthållandet av registerförteckningen är mycket personberoende, vilket som utgångspunkt inte är lämpligt.

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

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 rör framför allt praktisk tillämpning och effektivitet av de rutiner och strukturer som finns på plats. 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 kvalitén av innehållet i registerförteckningen och säkerställa att framför allt laglig grund är korrekt.

De personuppgiftsbehandlingar som i realiteten är godkända bör ha statusen godkänd i Draftit så att det inte uppstår några frågetecken.

Slutligen vad gäller risknivåerna för varje behandling kan det vara värt att ta i beaktande att nuvarande informationsklassning fokuserar på att klassa system och inte information. Det kan inte uteslutas att vissa behandlingar kan ha en högre risknivå än vad som gäller generellt för ett system och att det kan finnas ett värde att i alla fall identifiera risknivån för vissa prioriterade behandlingar inom bland annat HR.

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. Vad gäller rutiner för personuppgiftsincidenter finns numera en lokal rutin för personuppgiftsincidenter. Ett arbete har även påbörjats gällande nomenklatur för styrdokument.

En brist som kan påpekas gäller regler och rutiner kring e-post (detta påpekades även i årsrapporten för 2021). Gällande gallring av personuppgifter finns en instruktion för arkiv och gallring enligt GDPR som dock inte tar upp något specifikt gällande e-post.

Det finns även regler för elektronisk post i Stockholm stad som endast innehåller en mening om att ta hänsyn till GDPR när ett e-postmeddelande innehåller personuppgifter. Nuvarande dokumentation bör därför utökas med mer konkreta instruktioner för hur de anställda ska förhålla sig till personuppgifter i e-post.

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.

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
x	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

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

Den del som bedöms bör åtgärdas är regler och rutiner kring e-posthantering. DSO har inte tagit del av någon dokumentation som särskilt adresserar regler kring hur personuppgifter ska hanteras i e-post.

3.2.5 DSO ger råd och rekommendationer till PUA

Ser man till IMY:s rapport om anmälda incidenter så är så kallade felskick (bland annat att e-postmeddelanden skickas till fel mottagare) den vanligaste typen av incident. Senaste årets tillsynsbeslut visar även att det finns stora brister kring hanteringen av personuppgifter i e-postmeddelanden hos de aktörer som har varit föremål för tillsyn. Det är därför av stor vikt att verksamheten

är medveten om hur personuppgifter får användas när e-post skickas. Rekommendationen är därför att sådan dokumentation upprättas.

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 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.

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 2023 som har varit i behov av informationsklassning. Ett system har fasats ut sedan förra året.

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.

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 skrivbordskontroll.

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. Vid kontroll av denna lista och registerförteckningen är det rimligt att anta att de behandlingar där konsekvensbedömningar behöver genomföras har identifierats.

DSO har under arbetet med årsrapporten lyft frågan gällande behovet av konsekvensbedömning inom biblioteksverksamheten. Dataskyddssamordnaren har uppgett att verksamheten inte tagit ställning till om det behövs någon sådan än.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Under 2023 har konsekvensbedömning genomförts gällande behandlingen *rekrytering och casting.* För behandlingen *HR-rehab* har ett beslut tagits att denna behandling ryms inom de konsekvensbedömningar som gjort inom övriga behandlingar inom HR-processen och att någon egen konsekvensbedömning för denna inte är nödvändig.

DSO konstaterar 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.

Dataskyddsamordnaren har uppgett att en ansökan om utökad kamerabevakning har lämnats in och om tillstånd ges kan det bli aktuellt att uppdatera nuvarande konsekvensbedömning.

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 inte tagit hänsyn till kvaliteten och innehåller i de faktiska konsekvensbedömningarna, utan risken har främst satts utifrån nyckeltal kopplade till kontrollfrågorna. Sett till riskerna utifrån det perspektivet har inga större identifierats, utan verksamheten har kontroll och dokumentation över de behandlingar som kräver en konsekvensbedömning och reviderar även dessa bedömningar

årligen. DSO har emellertid uppmärksammat att någon risk – eller konsekvensbedömning inte har gjorts för biblioteksverksamheten.

3.4.5 DSO ger råd och rekommendationer till PUA

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

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	1 begäran om registerutdrag. Begäran om rättelse och radering kommer löpande.
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	Samtliga begäran om registerutdrag. Övriga 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 året har det kommit in en (1) 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.

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

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?	1
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
x	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	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 säkerhetsincident i allmänhet och en personuppgiftsincident i synnerhet är bristfällig och därmed anmäls inte sådant som borde anmälas. Det får därför antas att det finns ett mörkertal gällande inträffade personuppgiftsincidenter.

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 som talar för detta 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.

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 stor risk eftersom verksamheten inte har kontroll över denna fråga.

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

gällande e-posthantering för att kontrollera om det kan förekomma personuppgiftsincidenter inom e-post som inte upptäcks.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Personuppgiftsincidenter
- Uppgiftsminimering och lagring
- Registerförteckning
- Registrerades rättigheter

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

Personuppgiftsincidenter

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

Slutsatsen från granskningen av personuppgiftsincidenter var att KHST besitter god kunskap om personuppgiftsincidenter men

kunskapen besitts av få roller och är inte jämnt fördelad i organisationen.

Rekommendation från DSO var att hålla en utbildning för organisationen om vad en personuppgiftsincident är samt hur de anmäls. Vidare rekommenderades att en mall upprättas som enkelt kan fyllas i för att analysera och bedöma om det är sannolikt att personuppgiftsincidenten kommer att medföra en risk för de registrerades rättigheter och friheter. DSO rekommenderade slutligen att det bör finnas en utpekad roll som kan ta över ansvar för att anmäla om det är så att dataskyddssamordnaren är borta.

Uppgiftsminimering och lagring

	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 gällande uppgiftsminimering och lagring var att KHST har god kunskap och ett strukturerat arbetssätt med rutiner och beskrivningar gällande uppgiftsminimering och gallring. En brist som noterades var att gallringsrutiner för de personuppgifter som inte omfattas av arkivlagen eller utgör allmänna handlingar saknades.

Rekommendation från DSO var att upprätta en lokal rutin för uppgiftsminimering och gallring samt att gå igenom angivna tidsfrister för gallring i registerförteckningen och justera i de behandlingar som saknade angivna tidsfrister.

Efter granskningen har samtliga behandlingar justerats och tidsfrister har lagts in. Vad gäller rutin för uppgiftsminimering och gallring har ett nytt styrdokument upprättats (arkivhandbok) som innehåller rutiner för gallring. Utifrån att justeringar har gjorts har risken sänkts från granskningstillfället och bedöms numera vara enligt kategori grön.

Registerförteckning

	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

Vid granskning av registerförteckningen identifierades vissa brister och DSO lämnade följande rekommendationer:

1. Ange mottagare av personuppgifter.
2. Ange den rättsliga grunden för tredjelandsöverföringen.
3. Det bör läggas till uppgifter om gallring i registerförteckningen.
4. Det bör upprättas ett register över de behandlingar där KHST agerar personuppgiftsbiträde.
5. Kategorier av registrerade bör samlas i en kolumn för att skapa tydlighet.
6. Det finns många tomma kolumner och några skulle kunna tas bort.
7. Det saknas namn och kontaktuppgifter till dataskyddsombudet.
8. Se över de tekniska och organisatoriska säkerhetsåtgärderna.

Åtgärder har vidtagits efter granskningen men med hänsyn till den riskbedömning som gjorts under de obligatoriska granskningsområdena så är bedömningen att det finns identifierade brister som bör åtgärdas.

Registrerades rättigheter

	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

Vid granskning av de registrerades rättigheter var slutsatsen att det krävs att rutiner för att tillgodose den registrerades rättigheter upprättas samt att det är viktigt att den registrerade informeras på ett tydligt sätt i rätt tid och att informationen finns lättillgänglig.

Efter granskningen har information till de registrerade på webbplatsen uppdaterats samt personuppgiftspolicyn.

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

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
x	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	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.

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:

- Hantering av personuppgifter inom HR
- Hantering av personuppgifter inom kommunikation (med fokus på uppgifter som kommuniceras antingen på sociala medier eller på intranätet)
- Hantering av personuppgifter i e-post (med fokus på kundtjänst)

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

Känsliga och extra skyddsvärda personuppgifter inom HR

Inom HR hanteras en stor mängd känsliga och skyddsvärda personuppgifter. Det är därför av stor vikt att det finns tydliga rutiner kring hur personuppgifter inom HR ska hanteras samt att personalen som hanterar dessa personuppgifter har en god kunskap kring regelverket med hänsyn till den risk som föreligger om dessa personuppgifter hanteras felaktigt.

För att kunna genomföra granskningen kommer DSO att behöva tillgång till relevanta dokument samt att tid sätts av hos relevanta kontaktpersoner. Det kan även finnas behov av att få insyn i hanteringen i HR-system.

Granskningen kommer att kunna belysa hanteringen av känsliga och integritetskänsliga personuppgifter inom HR och därmed ge KHST en bra kartläggning över eventuella höga risker.

Hantering av personuppgifter inom kommunikation

Kommunikationsavdelningen hanterar oftast personuppgifter i stor utsträckning. Med hänsyn till den spridning en publicering kan få samt med hänsyn till maktobalansen som kan föreligga mellan den personuppgiftsansvarige och den vars personuppgifter som används i kommunikationen är det av stor vikt att det finns tydliga riktlinjer och en medvetenhet bland de anställda som jobbar med dessa frågor kring bestämmelser om integritet och dataskydd.

Granskningen kommer att kunna kartlägga eventuella integritetsrisker med potentiellt stor spridning (och därmed en högre risk) och ge KHST möjlighet att oftast med relativt enkla medel vidta åtgärder med stor effekt på riskbilden.

Hantering av personuppgifter inom e-post

I en verksamhet som inte i sig har som kärnverksamhet att hantera stora mängder personuppgifter är e-post det system där personuppgifter hanteras i stor utsträckning varje dag och oftast utan att den anställda reflekterar över vad för personuppgiftsbehandling som sker. Såsom har angetts under 3.2.5 så är e-post också en av de vanligaste källorna till incidenter och det är inte ovanligt att personuppgifter i e-postsystem inte gallras i enlighet med regler och rutiner. Det är viktigt att anställda är införstådda med hur personuppgifter får hanteras när de skickar e-post.

Granskningen kommer att kunna kartlägga eventuella risker gällande behandlingen av personuppgifter som inte följer de grundläggande principerna samt eventuella behov av säkerhetsåtgärder som kan behöva vidtas.

7 Övrigt att rapportera

7.1 Sammanfattning

DSO noterar att det föreligger vissa risker gällande granskning av behörighetsloggar samt det starka personuppgiftsberoendet som finns gällande dataskyddsarbetet. DSO noterar dock även att dataskyddsarbetet har prioritet och ständigt utvecklas och förbättras.

7.2 Syfte

Under denna punkt tas övriga punkter upp som inte passar in i övriga delar av rapporten. Syftet är att lyfta övriga aspekter som kan vara bra för den personuppgiftsansvarige att veta.

7.3 Övriga observationer

Åtkomst till behörighetsloggar avseende mailloggar

Denna fråga togs upp även i förra årets årsrapport där det konstaterades att det saknades tydliga processer hur det säkerställs att reglerna och rutinerna kring beställning och sammanställning av behörighetsloggar följs. Inga åtgärder har skett sedan förra året och kritiken kvarstår därför.

Systematiskt dataskyddsarbete och personberoende

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.

7.4 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att hanteringen kring granskning av loggar ses över.

Vidare är rådet att KHST ser över möjligheten att utöka sitt systematiska dataskyddsarbete genom att utse kontaktpersoner för dataskydd ute i verksamheten.