Stockholms stad

GDPR Årsrapport

År 2023

Kulturnämnden

GDPR årsrapport
2023

Dnr: KUL 2023/1958
Utgivningsdatum: 2024-01-23
Kontaktperson: Alexandre Emonide

1 Bakgrund

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

Enligt GDPR är varje nämnd och bolagsstyrelse inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att en 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 GDPR utnämnt ett Dataskyddsombud (”DSO”). DSO har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport syftar till att redogöra för de granskningar som gjorts under året. Rapporten avslutas med rekommendationer för det fortsatta dataskyddsarbetet.

Innehåll

2 Sammanfattning

DSO lämnar följande årsrapport. Denna rapport är sammanställd av DSO i syfte att ge personuppgiftsansvarig (PUA), i kulturförvaltningen fall är det kulturnämnden, en redogörelse för hur dataskyddsarbetet har genomförts på kulturförvaltningen under 2023. Kulturförvaltningen har viktiga delar som behöver komma på plats gällande dataskyddsarbetet. Det finns en registerförteckning i DraftIt som behöver uppdateras löpande. En stor brist är revidering av styrdokument som leder till bristande kvalitet i hur verksamheten utför aktiviteterna. Vidare behövs det tydliga rutiner för hur dataskyddsarbetet ska ske löpande i verksamheten.
En annan brist är avsaknad av konsekvensbedömningar där en insats har gjorts under 2023, men bör följas upp under 2024. En utbildningsinsats är planerad under våren 2024.

2.1 Översiktlig bedömd status för rapporteringsområden

Registerförteckning		X		
Styrdokument		X		
Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar		X		
Konsekvensbedömningar		X		
Individens rättigheter	X			
Personuppgiftsincidenter		X		

(För specificering se respektive avsnitt)

3 Obligatoriska rapporteringsområden

Denna årsrapport redogör för sex obligatoriska rapporteringsområden. Dessa områden ska ses över årligen av personuppgiftsansvarig (”PUA”) i syfte att efterleva dataskyddsförordningen.

De obligatoriska rapporteringsområdena är följande

- registerförteckning
- styrdokument
- tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar
- konsekvensbedömningar
- individens rättigheter och personuppgiftsincidenter
- Personuppgiftsbiträdesavtal

Nedan redogörs för kulturförvaltningens status och Dataskyddsombudet slutsatser samt rekommendationer.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	38
Har verksamheten rutiner som möjliggör att nya/förändrade personuppgiftsbehandlingar registreras?	Ja, Arbetet pågår
Bedöms registerförteckningen vara fullständig?	Delvis
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

Förteckning på behandlingar, även kallad registerförteckning eller behandlingsregister, är ett direkt lagkravkrav enligt GDPR. Kravet innebär att samtliga behandlingar av personuppgifter ska kartläggas i en förteckning/register. Informationen i förteckningen/registret ska hållas uppdaterad, aktuell och komplett och granskas av DSO. Syftet med detta avsnitt är att granska kulturförvaltningens förteckning/register.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats
I dagsläget finns det 38 personuppgiftsbehandlingar registrerade i registerföreteckningen.

DSO kontrollerar om nödvändiga uppdateringar gjorts
Registerförteckningen uppdateras inte så ofta som är önskvärt. Små justeringar är gjorda under året och registerförteckningen uppdateras kontinuerligt och förvaltningen har rutiner för att uppdatera den.

DSO bedömer hur fullständig registerförteckningen är
Registerförteckningen är omfattande men då den inte uppdateras regelbundet är den inte fullständig. Detta på grund av vissa behandlingar är i en ständig aktiv process i verksamheten. Vissa

behandlingar är ofullständiga. Till exempel att administrera ateljékö och ateljébostad, hantera subventioner för kulturutbud m.fl. Det saknas exempelvis beskrivning av tydligt och specifik ändamål, rättslig grund, gallringsdatum och det finns ingen konsekvensbedömning kopplad till registreringen.

Kulturförvaltningen har i ett par omgångar genomfört inventeringar av sina personuppgiftsbehandlingar i Draftit. Sammanlagt bedöms registret vara komplett även om majoriteten av inventeringar finns inaktiverade.

Dåvarande DSO har i juni 2023 gått genom alla behandlingar och angett både en kommentar och gjort en riskbedömning. Majoriteten av behandlingar har fått medelhög risk eftersom de behöver kompletteras och enligt vad DSO kan se i DraftIt finns det två behandlingar som har fått hög risk eftersom de behöver ses över. Det är kameraövervakning och söka Kollo. En kommentar från dåvarande DSO gällande att söka Kollo lyder: Personuppgiftsbehandlingen är ej tillräckligt beskrivet. Det saknas exempelvis beskrivning av tydligt och specifik ändamål, rättslig grund behöver motiveras samt vilka leverantörer man anlitat för att anordna aktiviteter för kollo. Inventeringen behöver kompletteras med mer detaljer i alla flikar.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring
Det saknas tydliga rutiner för hur, när och av vem registerförteckningen ska uppdateras. I dagsläget tycks uppdateringar ske främst på uppmaning från DSO.

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

3.1.5 DSO ger råd och rekommendationer till PUA

Fortsätt arbetet med att komplettera registerförteckningen och se över behandlingar som bedöms ha en hög risk. Registerförtekningen bedöms som komplett eftersom information har samlats in både i aktiva behandlingar och i inaktiva behandlingar.

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?	Delvis
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Ja
Är dokumenten uppdaterade?	Nej, inte allt
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Det finns en funktion som ansvarar för detta.

3.2.2 Syfte

Exempel på styrdokument är, mall för personuppgiftsbiträdesavtal, incidenthanteringsrutin och rutin för registerutdrag. Styrdokument ska finnas nedtecknade, beslutade och kommunicerade. Genom styrdokument kommuniceras till medarbetarna vad som förväntas av dem samt information om regler, ramar och förutsättningar och stöd för att upprätthålla kunskapen över tid och tillämpa den på ett konsekvent sätt. Syftet med detta avsnitt är att granska kulturförvaltningens styrdokument.

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?
Styrdokument finns framtagna centralt och kan anpassas till Kulturnämndens verksamhet vid behov.

Kulturförvaltningen har de styrande dokument på plats som dataskyddsförordningen föreskriver och som Stadsledningskontoret (SLK) uppmanar till. I en del fall finns centrala dokument och mallar framtagna av SLK, dessa har i viss mån anpassats till kulturförvaltningens verksamhet. De styrdokument och mallar som finns är samlade och tillgängliga för kulturförvaltningens medarbetare i en gemensam katalog.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet
DSO bedömer att centrala styrdokument är fullt tillräckliga och att de styrdokumenten för nämndens verksamhet kan uppdateras och revideras under 2024. Avsaknaden av tydliga rutiner och en otydlig ansvarsfördelning gör att dataskyddsarbetet riskerar att bli eftersatt inom vissa områden. Den största utmaningen i kulturförvaltningens dataskyddsarbete är att få till dessa rutiner på plats och att göra dataskyddsfrågorna till en integrerad del av den ordinarie verksamheten.

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

3.2.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar en översyn av samtliga styrdokument görs år 2024 för att identifiera vilka dokument som behöver kompletteras eller tas fram.

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?	Alla
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 Syfte

Tekniska och organisatoriska säkerhetsåtgärder är grunden till ett bra informationssäkerhetsarbete. Tekniska och organisatoriska säkerhetsåtgärder ska därför vara en del av organisationens arbete.

Tekniska säkerhetsåtgärder innefattar främst IT-säkerhet och systemsäkerhet. Organisatoriska säkerhetsåtgärder innefattar det systematiska GDPR-arbetet i form av rutiner, instruktioner analyser och regelefterlevnad.

Syftet med detta avsnitt är att granska kulturförvaltningens tekniska och organisatoriska säkerhetsåtgärder samt att ge rekommendationer kring det fortsatta arbetet.

3.3.3 Resultat

3.3.4 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

3.3.5 DSO ger råd och rekommendationer till PUA

Fortsätt arbetet med att komplettera behandlingsregistret löpande med information om tekniska och organisatoriska säkerhetsåtgärder. Samtliga personuppgiftsbehandlingar är klassade.

3.4 Konsekvensbedömningar

Fråga/kontroll	Svar
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?	Rutin för tröskelanalys är framtagen
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?	Ja, arbetet pågår
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd genomförs samt genomfört detta?	Arbete pågår
Finns det en ändamålsenlig mall samt för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?	Ja det ska finnas.

3.4.1 Sammanfattning

3.4.2 Syfte

Syftet med att göra konsekvensbedömningar är att förebygga risker för att skydda de registrerade och att efterleva GDPR. En konsekvensbedömning är en bedömning av de konsekvenser som kan uppstå när man behandlar personuppgifter. I bedömningen tar man ställning till om risken är proportionerlig i förhållande till ändamålet med behandlingen av uppgifterna. Visar det sig att risken är för hög för att motivera ändamålet kan bedömningen resultera i att det inte går att genomföra behandlingen, alternativt ta fram åtgärder för att sänka risken. En konsekvensbedömning ska även genomföras om det föreligger risker då en behandling förändras.

Syftet med detta avsnitt är att granska kulturförvaltningens rutin för konsekvensbedömningar samt att ge rekommendationer kring det fortsatta arbetet.

3.4.3 Resultat

Kulturförvaltningen har deltagit vid flera konsekvensbedömningar under första halvan av 2023.

Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?
Nej, ingen övergripande genomgång har gjorts för att identifiera om det finns fler behandlingar som behöver konsekvensbedömmas. Arbetet med att identifiera personuppgiftsbehandlingar som kräver en konsekvensbedömning pågick löpande under första halvan av året. För perioden september-december 2023 har inga personuppgiftsbehandlingar som kräver en konsekvensbedömning identifierats.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?
För perioden september-december 2023 har inga högriskbehandlingar identifierats.

Är de genomförda konsekvensbedömningarna aktuella?
För perioden september-december 2023 har inga högriskbehandlingar varit aktuella.

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

3.4.5 DSO ger råd och rekommendationer till PUA

Rutin för tröskelanalys har tagits fram och två konsekvensbedömningar har gjorts enligt stadens mall. Även översyn av alla behandlingar har genomförts för att identifiera behandlingar som kräver en konsekvensbedömning. Översynen resulterade i en behandling som enligt tröskelanalysen hade en rekommendation om att göra en fullständig konsekvensbedömning. Konsekvensbedömningen för den behandlingen gjordes våren 2023. DSO rekommenderar ett fortsatt arbeta med detta görs under första kvartalet 2024.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?	Ja
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	0
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	0

3.5.2 Syfte

Individens rättigheter regleras i flera artiklar i GDPR. Några rättigheter som kan nämnas är den registrerade rätt att begära och få registerutdrag, rätt till rättelse samt rätt till radering.

Syftet med detta avsnitt är att granska kulturförvaltningens dokumentation och arbetsmaterial gällande individens rättigheter samt att ge rekommendationer kring det fortsatta arbetet.

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

Ja, det har kulturförvaltningen.

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

3.5.5 DSO ger råd och rekommendationer till PUA

DSO har inget att rekommendera.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur säkerhetsställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftincident?	Ja rutin finns, dock behöver kunskapen höjas. Anställda rapporterar till chef, rutin håller på att ändras så att anställda kan rapportera direkt i IA
Finns det rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter samt följs dessa?	Ja
Hur många personuppgiftsincidenter har anmälts IMY?	0
Hur många personuppgiftsincidenter har dokumenterats?	4

3.6.2 Syfte

Att identifiera och hantera personuppgiftsincidenter är ett direkt krav i GDPR. Det är även viktigt att aktivt arbeta med att förebygga

personuppgiftsincidenter för att spara tid och resurser samt för att bygga en riskmedveten säkerhetskultur i verksamheten.

Syftet med detta avsnitt är att granska kulturförvaltningens rutiner och processer gällande personuppgiftsincidenter samt att ge rekommendationer kring det fortsatta arbetet.

3.6.3 Resultat

Hur väl förmår verksamheten att rapportera personuppgiftsincidenter i tid till Integritetsskyddsmyndigheten?
Nuvarande rutin för rapportering av personuppgiftsincidenter behöver ses över och eventuellt förtydligas i verksamheten.

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

3.6.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att arbeta med rutinen för personuppgiftsincidenthantering tillsammans med medarbetarna i samband med en föreläsning/workshop under våren 2024. För att göra rutinen mer känd i verksamheten, samt få en ökad kunskap och förståelse för vad en personuppgiftsincident är.
Ett arbete med utbildning/informationsinsatser planerades under våren 2024.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Personuppgiftsbiträdesavtal
- Styrdokument

4.2 Syfte

En av DSO:s viktigaste uppgifter är att övervaka verksamhetens efterlevnad av dataskyddsförordningen. En central del av det arbetet 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

4.3.1 Personuppgiftsbiträdesavtal

	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

Förutom de områden som redan tagits upp i denna rapport har en genomgång av kulturförvaltningens personuppgiftsbiträdesavtal (PUB-avtal) gjorts av DSO. Kulturförvaltningen har PUB-avtal på plats för det personuppgiftsbehandlingar som kräver det. Kulturförvaltningen använder främst Stadsledningskontorets (SLK) PUB-avtalsmall. En del av dessa avtal bör ses över och uppdateras.

4.3.2 Styrdokument

	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

Arbete pågår.

4.4 DSO ger råd och rekommendationer till PUA

Det är okänt om några riskkartläggningar har gjorts under första halvan av året 2023.
Det behövs ses över och arbetas mer aktivt med rutiner och utbildningsinsatser.

5 Risker inom dataskydd

5.1 Sammanfattning

Det är okänt om några riskkartläggningar har gjorts under första halvan av året 2023. Avsaknaden av tydliga rutiner och en otydlig ansvarsfördelning gör att dataskyddsarbetet riskerar att bli eftersatt inom vissa områden. Den största utmaningen i kulturförvaltningens dataskyddsarbete är att få till dessa rutiner på plats och att göra dataskyddsfrågorna till en integrerad del av den ordinarie verksamheten.

Det behövs ses över och arbetas mer aktivt med rutiner och utbildningsinsatser.

Den största utmaningen i kulturförvaltningens dataskyddsarbete är användningen av konton i sociala medier. Kulturförvaltningen behöver se över sociala medier konton i verksamheterna och minska antalet konton.

Kulturförvaltningen har tagit bort lagliga grund – samtycken, vid publicering av bild, film- och ljudupptagningar på sociala medier. Förvaltningen kommer istället använda allmänt intresse som laglig grund och där de som på olika sätt publiceras får ta del av information om vad som händer vid publicering på sociala medier via en informationsblankett.

5.2 Syfte

Verksamheten har ansvar för att göra vissa typer av riskanalyser, så som konsekvensbedömningar och informationsklassningar, men dessa ger inte en heltäckande bild av personuppgiftsriskerna i verksamheten. DSO behöver som underlag för sin egen planering och sitt löpande arbete ha kontinuerlig överblick över dessa risker, i verksamhetens samtliga personuppgiftsbehandlingar. Exempelvis krävs en sådan överblick för att kunna välja ut vilka områden som bör granskas under det kommande året eller för att avgöra vilka råd som DSO behöver lämna till verksamheten om dataskyddsåtgärder som behöver vidtas.

5.3 Resultatet av riskkartläggningen

Sociala medier konton

	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

Risker har identifierats i användningen av sociala medier konto inom förvaltningen och publicering av fotografier. Kommentarer till riskerna finns dokumenterade i förvaltningens registerförteckning i Draftit.

5.4 DSO ger råd och rekommendationer till PUA

Sociala medier konton
DSO rekommenderar ett fortsatt arbete med att se över användningen av sociala medier konton i verksamheterna och minska antalet konton. Kulturförvaltningen har tagit bort samtycke för fotografering och har nu allmänt intresse som laglig grund. Det finns nu en informationsblankett för att informera om att viss överföring görs utanför EU/ESS. Den här risken har nu sänks från hög risk till medel risk i DraftIt.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Styrdokument
- Utbildningsinsatser
- Årshjulsplanering för ett mer systematiskt och kontinuerligt dataskyddsarbete.

6.2 Syfte

Som nämnts ovan är det granskande arbetet en av DSOs viktigaste uppgifter. Eftersom DSO ofta har begränsat med tid, behöver granskningsplanen för det nya året utformas med eftertanke. Som en tumregel bör två-tre granskningar ses som en rimlig granskningsinsats under ett verksamhetsår. Granskningsområdena bör lämpligen väljas utifrån ett riskbaserat synsätt, det vill säga att fokus bör ligga på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Därigenom åstadkoms en röd tråd i dataskyddsarbetet från ett verksamhetsår till nästa samtidigt som de största riskerna elimineras eller åtminstone sänks till en mer acceptabel nivå.

6.3 Planerade granskningar

6.3.1 Styrdokument

DSO rekommenderar en översyn av samtliga styrdokument görs år 2024 för att identifiera vilka dokument som behöver kompletteras eller tas fram.

6.3.2 Utbildningsinsatser

Ett arbete med utbildning/informationsinsatser planerades under våren 2024, för att öka kunskapen och förståelsen för vad en personuppgiftsincident är.

6.3.3 Årshjulsplanering för ett mer systematiskt och kontinuerligt dataskyddsarbete

Årshjulsplanering bygger på att arbetet inom dataskyddet delas upp i ett årshjul, där varje månad är indelad i ett fokusområde som DSO kan fokusera på. I årshjulet delas arbetsuppgifterna upp i löpande aktiviteter som utvärderas, granskas och förbättras. Årshjulet är ett effektivt sätt att strukturera arbetet. Det är även ett bra sätt att fördela arbetet mellan DSO och Dataskyddsorganisationen. Genom

att arbeta strukturerat med årsrapport och granskning kan man följa kulturförvaltningens progress under en längre tid.

7 Övrigt att rapportera

7.1 Syfte

Detta avsnitt används för att lyfta fram observationer som gjorts men som inte på ett naturligt sätt kunnat presenteras under övriga granskningsområden.

7.2 Övriga observationer

Observation 1
Samarbetet med informationssäkerhetssamordnaren har fungerat mycket bra. Då DSO får mycket frågor föreslås ett förbättrat arbetssätt för att effektivisera arbetssättet och minska arbetsbördan för DSO.

7.3 DSO ger råd och rekommendationer till PUA

Rekommendation 1
En genomgång av GDPR arbetet bör hållas inför kulturförvaltningens ledningsgrupp där man lyfter fram förvaltningens utmaningar avseende GDPR och exempelvis sociala medier.

Rekommendation 2
DSO rekommendation till nästa årsrapport är att det läggs in ytterligare ett rapporteringsområde - Överföring till tredje land
Förslag på frågor:

- Har personuppgiftsansvarig identifierat de tredjelandsöverföringar denne utför?
- Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?
- Har nödvändig bedömning, så kallad ”Transfer Impact Assessment (TIA), gjorts avseende de tredjelandsöverföringar som utförs?