Stockholms stad

GDPR Årsrapport

År 2023

Servicenämnden

GDPR årsrapport
2023

Dnr: SF 2024/82
Utgivningsdatum: 2023-12-29
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 Serviceförvaltningen fall är det Servicenämnden, en redogörelse för hur dataskyddsarbetet har genomförts på Serviceförvaltningen under 2023. Serviceförvaltningen har viktiga delar som behöver komma på plats gällande dataskyddsarbetet. Det finns ett behandlingsregister i Excel 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

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

Nedan redogörs för Serviceförvaltningens status och DSO slutsatser samt rekommendationer.

3.1 Behandlingsregistret

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	828
Har verksamheten rutiner som möjliggör att nya/förändrade personuppgiftsbehandlingar registreras?	Ja
Bedöms behandlingsregistret vara fullständig?	Ja, kan utvecklas
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

Förteckning på behandlingar, även kallad Behandlingsregistret eller registerförteckning, är ett direkt lagkravkrav enligt GDPR. Kravet innebär att samtliga behandlingar av personuppgifter ska kartläggas i ett behandlingsregister. Informationen i behandlingsregistret ska hållas uppdaterad, aktuell och komplett och granskas av DSO. Syftet med detta avsnitt är att granska Serviceförvaltningens behandlingsregister.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

Antal registrerade behandlingar I dagsläget finns 828 personuppgiftsbehandlingar registrerade i behandlingsregistret.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Under året har behandlingsregistret kompletterats med tekniska och organisatoriska säkerhetsåtgärder för de behandlingar som saknade beskrivning.

DSO bedömer hur fullständig behandlingsregistret *är*

I nuläget ser registerförtekningen ut att vara fullständig. Kan förbättras under 2024

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Registret uppdateras kontinuerligt och förvaltningen har rutiner för att uppdatera den. Kommentar till tidigare GDPR rapport 2022: Rutin för tröskelanalys har tagits fram och befintliga behandlingar kommer att gås genom för att identifiera vilka omfattas av krav på konsekvensbedömning.

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 behandlingsregistret med tekniska och organisatoriska säkerhetsåtgärder samt information om konsekvensbedömning.

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?	Stadens gemensamma styrdokument uppdateras centralt. Arbetet pågår
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 Serviceförvaltningens styrdokument.

3.2.3 Resultat

Serviceförvaltningen innehar följande styrdokument:

- Rutin för personuppgiftsincidentrapportering,
- Rutin för konsekvensbedömning, samt rutin för tröskelanalys
- Hantera begäran av registerutdrag - information
- Publicering av bilder innehållande personuppgifter – servicenämndens rutin
- Fotografering personuppgift info till registrerade

- Riktlinje för personuppgifter i system
- Lokal anvisning Serviceförvaltningen Informationssäkerhet
- Hanteringsrutin för informationssäkerhets-incidenter
- Rutin vid nytt Dataskydsombud

Finns lämplig styrande dokumentation på plats?

Styrdokument finns framtagna centralt och kan anpassas till Servicesnämndens verksamhet vid behov.
Servicesförvaltningen 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 Servicesförvaltningens verksamhet. De styrdokument och mallar som finns är samlade och tillgängliga för Servicesförvaltningens 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.

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

Serviceförvaltningen har styrdokument som inte är uppdaterad och anpassad till Serviceförvaltningens verksamhet. Det finns också vissa frågetecken kring hur kännedomen kring dessa styrdokument är i organisationen. Den dataskyddsorganisation som finns fastställd behöver uppdateras och vidareutvecklas för att kunna användas praktiskt i verksamheten.

3.2.5 DSO ger råd och rekommendationer till PUA

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

- Rutin för personuppgiftsincidentrapportering,
- Rutin för konsekvensbedömning, samt rutin för tröskelanalys
- Hantera begäran av registerutdrag - information
- Publicering av bilder innehållande personuppgifter – servicenämndens rutin
- Fotografering personuppgift info till registrerade
- Riktlinje för personuppgifter i system
- Lokal anvisning Serviceförvaltningen Informationssäkerhet
- Hanteringsrutin för informationssäkerhets-incidenter
- Rutin vid nytt DSO

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?	Arbetet pågår
Är klassade personuppgiftsbehandlingar aktuella?	Ja, delvis

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 Serviceförvaltningens tekniska och organisatoriska säkerhetsåtgärder samt att ge rekommendationer kring det fortsatta arbetet

3.3.3 Resultat

Serviceförvaltningen har koll på de uppgifter som finns i behandlingsregistret och uppgifterna är klassade utifrån den klassificieringsstruktur som Stadsarkivet har. Dem är dock inte klassificerade utifrån en informationsklassning pga. att det inte finns möjligheter att göra det då Serviceförvaltningen antingen är personuppgiftsbiträde eller hanterar andras information och inte är informationsägare och arbetar i andras system. Serviceförvaltningen är oftast inte likaså systemägare.

En anvisning arbetas fram under året 2023 som bland annat ska behandla registerförteckning, informationsklassning, riskanalys, tröskelanalys och konsekvensbedömning.
I övrigt är alla personuppgiftsbehandlingar har informationsklassats och är aktuella.

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

DSO rekommenderar att fortsätta arbetet med att komplettera behandlingsregistret med information om tekniska och organisatoriska säkerhetsåtgärder. I anvisningen bör man införa en checklista på behandlingar för att visa att man till exempel har informationsklassat, eller om det innehåller känsliga- och eller skyddsvärda personuppgifter. Detta för att tydligt se vart verksamheten behöver arbeta vidare med.

Stäm även av med informationssäkerhetssamordnare vilka system/behandlingar är informationsklassade.

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?	Arbete pågår

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 Serviceförvaltningens rutin för konsekvensbedömningar samt att ge rekommendationer kring det fortsatta arbetet.

3.4.3 Resultat

Serviceförvaltningen 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

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?	2
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	1

3.5.1 Sammanfattning

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 Serviceförvaltningens 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 Serviceförvaltningen.

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?	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, se över rutinerna
Hur många personuppgiftsincidenter har anmälts IMY?	1
Hur många personuppgiftsincidenter har dokumenterats?	1

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 Serviceförvaltningens 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. Detta för att göra rutinen etablerade i verksamheten och höja medvetenheten om incidenthantering. Vidare har det förts diskussioner om att ersätta IA som rapporteringssystem för personuppgiftsincidenter, dock finns det i nuläget inga andra alternativ.
Ett arbete med utbildning/informationsinsatser planeras under våren 2024.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Personuppgiftsbiträdesavtal
- Styrdokument
- Personuppgiftincidenter

4.2 Syfte

DSO ska i sitt arbete göra återkommande granskningar av hur väl GDPR efterlevs i verksamheten. Resultaten av granskningarna ligger sedan till grund för vilka beslut verksamheten fattar 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 resultatet av granskningarna.

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 Serviceförvaltningens personuppgiftsbiträdesavtal (PUB-avtal) gjorts av DSO. Serviceförvaltningen har PUB-avtal på plats för det personuppgiftsbehandlingar som kräver det. Serviceförvaltningen använder främst Stadsledningskontorets (SLK) PUB-avtalsmall. En el 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.

4.3.3 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

Förutom de områden som redan tagits upp i denna rapport har en genomgång av Serviceförvaltningens personuppgiftincidenter, då det förekommit en hel del av samma art. DSO har observerat brister i rutiner kring persontransporter där blanketter med känsliga uppgifter har skickats per e-mail.
Serviceförvaltningen ser sig som personuppgiftsbiträde i detta fall, då de upphandlar åt de andra fack- och stadsdelsförvaltningarna.
Det pågår fortfarande en dialog om vem som är Personuppgiftsbiträde respektive personuppgiftsansvarig med en av de tre leverantörerna.
Frågan är vem äger processen?

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 största riskerna inom dataskydd för Serviceförvaltningen har redan beskrivits i denna rapport. Avsaknaden av tydliga rutiner och en otydlig ansvarsfördelning gör att dataskyddsarbetet riskerar att bli eftersatt inom vissa områden. Den största utmaningen i Serviceförvaltningens dataskyddsarbete är att få till dessa rutiner på plats och att göra dataskyddsfrågorna till en integrerad del av den ordinarie verksamheten.

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

Som tidigare nämnts finns det på Serviceförvaltningen inom de flesta delar av dataskyddsområdet en bra grund att arbeta vidare från.

Bristande rutin kring persontransporter

	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

Se kommentarer och rekommendation under punkt 4.3.3.

Utbildningsinsatser

	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

5.4 DSO ger råd och rekommendationer till PUA

Utbildningsinsatser till målgrupper som arbetar mest med personuppgifter bör genomföras under våren. Under våren 2024 bör det planeras korta informationsinsatser på särskilda ledningsgrupper eller arbetsplatser. Det är avdelningschefernas ansvar tillsammans med DSO att det genomförs.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Styrdokument
- Personuppgiftsincidenter
- 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 styrdokument görs år 2024 för att identifiera vilka dokument som behöver kompletteras eller tas fram.
Följande styrdokument som bör kontrolleras:

- Rutin för personuppgiftsincidentrapportering,
- Rutin för konsekvensbedömning, samt rutin för tröskelanalys
- Hantera begäran av registerutdrag - information
- Publicering av bilder innehållande personuppgifter – servicenämndens rutin
- Fotografering personuppgift info till registrerade
- Riktlinje för personuppgifter i system
- Lokal anvisning Serviceförvaltningen Informationssäkerhet
- Hanteringsrutin för informationssäkerhets-incidenter
- Rutin vid nytt DSO

6.3.2 Personuppgiftsincidenter

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 Serviceförvaltningens progress under en längre tid.

7 Övrigt att rapportera

7.1 Övriga observationer

Observation 1

Serviceförvaltningen är den enda förvaltningen inom Stockholm stad som agerar som personuppgiftsbiträde för majoriteten av sina personuppgiftsbehandlingar åt andra förvaltningar. I regel är alla nämnder inom Stockholm stad egna personuppgiftsansvariga för sina behandlingar och Serviceförvaltningen är endast personuppgiftsansvarig för behandlingar som avser den egna verksamheten och egna anställda, alla andra behandlingar utförs på uppdrag av andra förvaltningar.

Det är av största vikt att Serviceförvaltningen får tydliga instruktioner för att behandla personuppgifter på uppdrag av andra nämnder. Denna otydliga PUA-PUB relation skapar oftast förvirring när personuppgiftsincidenter ska utredas, när PUB avtal ska tecknas och när ansvarsfrågan kommer upp i olika situationer.

Serviceförvaltningen håller på att ta fram en instruktion som ska vara gemensam för alla förvaltningar och den behöver förankras med nämnderna och staden centralt.

Observation 2

Samarbetet med dataskyddssamordnaren och informationssäkerhetssamordnaren har fungerat bra. Tyvärr har den korta tid som DSO haft gjort att samarbetet inte har kunnat fördjupas.

7.2 DSO ger råd och rekommendationer till PUA

Säkerställ att Serviceförvaltningen får tydliga instruktioner från andra personuppgiftsansvariga nämnder och att instruktionen är förankrat med staden centralt. Rollen som personuppgiftsbiträde behöver vara tydlig.

DSO rekommenderar att till nästa årsrapport 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?