Stockholms stad

Bilaga 4

GDPR Årsrapport

År 2023

Idrottsförvaltningen

GDPR årsrapport
2023

Utgivningsdatum: 2024-01-11
Kontaktperson: Alexandre Emonide

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 privatliv 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”). Dataskyddsombudet 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

Dataskyddsombudet lämnar följande årsrapport.
Denna rapport är sammanställd av DSO i syfte att ge personuppgiftsansvarig (PUA), i Idrottsförvaltningen fall är det Idrottsnämnden, en redogörelse för hur dataskyddsarbetet har genomförts på Idrottsförvaltningen under 2023. Idrottsförvaltningen 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 Idrottsförvaltningens status och Dataskyddsombudet slutsatser samt rekommendationer.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	93
Har verksamheten rutiner som möjliggör att nya/förändrade personuppgiftsbehandlingar registreras?	Arbetet pågår
Bedöms registerförteckningen vara fullständig?	Ja
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 Dataskyddsombudet. Syftet med detta avsnitt är att granska Idrottsförvaltningens förteckning/register.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

I dagsläget finns det personuppgiftsbehandlingar registrerade i registerföreteckningen.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Nödvändiga uppdateringar sker kontinuerligt.

DSO bedömer hur fullständig registerförteckningen är

Uppdatering av registerförteckning pågår och identifierade brister kommer att åtgärdas.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Det pågår ett arbete med att ta fram lämpliga rutiner för detta.

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 kontinuerligt. Registerförtekningen bedöms som komplett.

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, delvis
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja, Administrativa avdelningen

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 Idrottsförvaltningens styrdokument.

3.2.3 Resultat

Rapporteringen av området är tvådelad: dels ska DSO bedöma om verksamheten har styrdokument på plats, dels ska rapporteringen visa om dokumentationen innehållsmässigt håller en lämplig kvalitet, i vilket bland annat ingår att dokumentationen ska vara uppdaterad och aktuell. En brist inom detta område bör ses som en brist i förhållande till direkta lagkrav, men det finns fler nyanser av detta som bör lyftas fram till PUA. Bristande styrning på grund av att lämplig styrande dokumentation saknas leder ofta till bristande kvalitet i hur verksamheten utför aktiviteterna, men även till att verksamheten slösar värdefulla resurser när för många personer blir involverade i exempelvis en incidenthantering. Ytterligare ett exempel värt att nämna är att en analys görs om från grunden varje gång i stället för att ha styrdokument att utgå ifrån.

Idrottsförvaltningen innehar följande styrdokument som DSO på denna korta tid fick inblick i:

- Vägledning för personuppgiftsincident
- Stadsövergripna:
    - Riktlinje för incidenthantering
    - Överföring av personuppgifter till tredjeland

Finns lämplig styrande dokumentation på plats?

Idrottsförvaltningen har de styrande dokument på plats enligt ISAM. Dokumentation som finns är inte uppdaterad och anpassad till idrottsförvaltningens 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.

De styrdokument och mallar som finns är samlade och tillgängliga för idrottsförvaltningens medarbetare i en gemensam katalog.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

DSO bedömer att det bör göras en översyn av vilka styrdokument som saknas och vad som behövs revideras kommande år.

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?	Informationsklassningar är genomförda för förvaltningens lokala verksamhetssystem. 10 stycken. Dessa ska ses över igen under 2024. Utöver dessa har vi klassat 3 av Stadens system, Lisa och Agresso och Zoom samt tagit fram upphandlingskrav för 4 stycken nya system.
Är klassade personuppgiftsbehandlingar aktuella?	Dem är aktuella, arbete pågår för att se över dem.

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

3.3.3 Resultat

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

Fortsätt arbetet med att komplettera registerförteckningen i Draftit med information om tekniska och organisatoriska säkerhetsåtgärder. Stäm av med informationssäkerhetssamordnare vilka system/behandlingar är informationsklassade innan året är slut.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?	Rutin för tröskelanalys 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?	Ja
Finns det en ändamålsenlig mall samt för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?	Ja, behöver dock förtydligas

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

3.4.3 Resultat

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?	4
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	Ingen

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 Idrottsförvaltningens 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?

2 begäran om registerutdrag. Ingen av dessa har skickat in blankett. Därför inte åtgärdat.
1 begäran om radering. Inte skickat in blankett därför inte åtgärdat.
1 radering ur e-postlista. Åtgärdat efter ett första misslyckat försök. Totalt 52 dagar.

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

3.5.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att fortsätta arbeta fram ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade.

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.
Finns det rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter samt följs dessa?	1
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 Idrottsförvaltningens 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

Få granskningar genomfördes under perioden september-december 2023 eftersom DSO har haft en begränsad insyn i verksamheten såsom material De genomförda granskningarna är:

- Registerförteckning
- Styrdokument
- Registerutdrag

4.2 Syfte

En av DSOs viktigaste uppgifter är att övervaka verksamhetens efterlevnad av GDPR. 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 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

Komplettera registerförteckningen.

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 Registerutdrag

	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

4.4 DSO ger råd och rekommendationer till PUA

4.4.1 Styrdokument och registerutdrag

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

4.4.2 Registerförteckning

Fortsätt arbetet med att komplettera registerförteckningen och identifiera personuppgiftsbehandlingar som omfattas av krav på genomförande av konsekvensbedömning genom att göra tröskelanalys på befintliga personuppgiftsbehandlingar. Viktigt att man inte tappar fart i arbetet trots byte av DSO.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- Rutin för registerutdrag

5.2 Syfte

Verksamheten har ansvar för att göra vissa typer av riskanalyser, så som konsekvensbedömningar och informationsklassningar, dessa ger dock inte en heltäckande bild av personuppgiftsriskerna i verksamheten. DSO behöver 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 DSO ger råd och rekommendationer till PUA

Rekommendation 1
Utbildningsinsatser till målgrupper som arbetar mest med personuppgifter bör genomföras under våren. En informationsinsats för nämndens upphandlingsenhet ägde rum under våren 2023 och

det framgick då att det finns ett behov av att förtydliga vad som gäller kring tecknande av personuppgiftsbiträdesavtal. Under våren planerade och genomfördes korta informationsinsatser för särskilda ledningsgrupper eller arbetsplatser med dåvarande DSO. Denna insats ska fortsätta genomföras under våren 2024.

Rekommendation 2
I årsrapporten för 2022 framgår det att en granskning av personuppgiftsincidenter har genomförts. Den visade att rutinen för rapportering är ganska okänd i verksamheten. Rapporteringen görs i IA som är ett HR verktyg för arbetsmiljö och inte ett anpassat verktyg för rapportering av personuppgiftsincidenter. Fram till det att ett nytt arbetssätt för rapportering av personuppgiftsincidenter eller ett nytt verktyg införs behöver nuvarande rutin göras känd i verksamheten. Detta kan göras via utbildningsinsatserna som planeras till våren 2024.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Styrdokument
- Utbildningsinsatser – Personuppgiftsincidenter
- Registerförteckning och Konsekvensbedömningar
- Registerutdrag
- 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 Registerförteckning och Konsekvensbedömningar

Rutiner för tröskelanalys och konsekvensbedömning har tagits fram och konsekvensbedömningar gjordes enligt stadens mall under första kvartalet 2023 tillsammans med dåvarande DSO. Under första kvartalet 2024 kommer en större granskning och genomgång av registerförteckning och konsekvensbedömningar att göras för att se om de brister som beskrivits i denna rapport har åtgärdats. DSO kommer även att ha en rådgivande funktion under arbetet med att åtgärda bristerna.

6.3.4 Registerutdrag

Idrottsförvaltningen behöver se över rutin för registerutdrag.

6.3.5 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 Idrottsförvaltningens 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

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?