Stockholms stad

Bilaga 4

GDPR Årsrapport

År 2022

Idrottsförvaltningen

GDPR årsrapport
December 2022

Utgivningsdatum: 2022-12-30
Kontaktperson: Rosemarie Arnmark

1 Bakgrund

Denna rapport presenterar resultatet på årets granskning av efterlevnaden av Dataskyddsförordningen.

Rapporten är framtagen av dataskyddsombudet som nämnd eller bolagsstyrelse har utnämnt.

Målgrupp är beslutsfattare som skall fatta beslut om det kommande årets dataskyddsarbete. 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 nämnd/bolagsstyrelse uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

En annan målgrupp är medarbetare i den nämnd eller bolagsstyrelse som blivit granskad, som bistår dataskyddsombudet med information som ligger till grund för granskningen, och kvalitetssäkring att rätt information blivit granskad.

I Dataskyddsförordningen finns en stor mängd krav, tillämpliga krav har, i denna rapport, blivit indelad i granskningsområden. Granskningen innebär att dessa områden kontrolleras och bedöms i hur väl de möter lagens krav, och om det finns brister och vilka dessa brister i så fall är. Bristerna värderas utifrån de risker på dataskyddet som bristerna innebär. Även åtgärder föreslås för bristerna.
Granskningen är i sig krav från Dataskyddsförordningen, för att man skall mäta efterlevnad, kunna åtgärda brister och planera sitt förbättringsarbete.

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

Förklaringar i rapporten
I rapporten används så kallad trafikljus för att tydliggöra bedömd status för kontrollområdet. Här presenteras vad respektive färg motsvarar. Det innebär i realiteten att enbart status representerad av grön färg kan sägas vara godkänd status. För förbättringar bör fokus vara på att åtgärda brister som fått röd status omgående, brister som fått orange status bör planeras skyndsamt och brister som fått gul status kan planeras att genomföras i samband med andra närliggande insatser.

Trafikljusförklaring

	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
	Inga brister av nämnvärd betydelse identifierade

Innehåll

2 Sammanfattning av rapporten

I detta avsnitt kommenteras kort kring framsteg och översiktlig bedömd status.

Rapporten som helhet innehåller sammanfattningar och specificeringar. Den som i första hand vill läsa sammanfattning av granskning kan läsa Kapitel 2. I de följande kapitlen ges en fördjupad information av resultat av granskningar, bedömning och rekommendationer.

2.1 Framsteg under året

Under året har ett antal framsteg uppnåtts gentemot planering för förbättringsarbetet av efterlevnaden av Dataskyddsförordningen.

Under året har extern DSO tillsats som man delar med fem andra fackförvaltningar. Tanken är att det kan vara fördelaktigt med utomstående expertis, samt synergieffekter med en DSO som kan fånga styrkor hos enskilda förvaltningar som kan komma de övriga tillgodo.

En utbildningsinsats är planerad att genomföras under första kvartalet av 2023. Utbildningsinsatsen är avsedd att stärka de roller som har ansvarsområden på förvaltningen och stöttar den övriga organisationen i frågor som tangerar GDPR. Även här samordnat och gemensamt för förvaltningarna med tanke på synergi effekter. Även roller som objektansvariga och projektledare behöver få stärkt GDPR medvetenhet då de har ansvarspunkter för att upprätthålla och införa efterlevnadskraven i förvaltning och i projekt.

För att underlätta förståelse för konsekvensanalys, pågår ett arbete för att tydliggöra momentet Tröskelanalysen för att formellt definiera då konsekvensbedömning anses ej behöva genomföras.

2.2 Översiktlig bedömd status för rapporteringsområden

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

(För specificering se respektive avsnitt)

2.3 Sammanfattning föreslagna åtgärder till PuA från granskningar

- Ett viktigt fokus för 2023 bör vara att komplettera informationen i registerförteckningen
- Införa årsmässig genomgång av registerförteckningen, tydliggör ansvar på informationsägare.
- Kompletterande stöd för process där registerförteckning, informationsklassning riskanalys samt konsekvensbedömning ingår. Skapa mål för ett systematiskt och kontinuerligt arbetssätt, där informationsägare tar ansvar.
- Information om informationsklassning riskanalys och konsekvensbedömning är särskilt låg i registerförteckningen, 100 % saknas. Hög prioritet för komplettering rekommenderas. Även viktig information som säkerhetsåtgärder ligger på höga bristvärden.
- För styrdokument rekommenderas att en fastställd informationsägare finns för varje dokument och ett fält där datum för senaste uppdatering framgår.
- Bedömda brister för personuppgiftsincidenthanteringen är att det inte verkar vara klarlagt vilka personer som äger ansvaret för att lyfta personuppgiftsincidenten och vart man lyfter.
- Ytterligare brist för personuppgiftsincidenthanteringen verkar vara en mall som sammanfattar vilken information som ger bra bedömningsunderlag.
- Det verkar vara en brist i arbetet med att fastställa behovet av PuB avtal, alternativt enbart att uppdatera informationen i registerförteckningen.

2.4 Observationer

Observation 1

Dataskyddsarbetet är beroende av flera roller där rollen informationssäkerhetssamordnaren är central för att hålla ihop arbetet med informationsklassning och riskanalys, medan objekt-ansvarig ansvarar för behandlingen som har information om själva behandlingen och vilka personuppgifter som ingår.

Risk: Om inte samsyn kring ansvar och ägarskap upprättas kring dessa moment inom dataskyddsarbetet kan det innebära att det är svårt att höja kvalitén på dataskyddarbetet.

Observation 2

Under hösten har administrativ chef beställt kompletterande utbildning för de roller som behöver förstå dataskyddsdelarna i sitt eget ansvarsområde.
Utbildningen är planerad att genomföras under Q1 2023.

2.5 Sammanfattning rekommendationer till PUA för observationer

- Förutsättningar för nära samarbete mellan DSO, informationssäkerhetssamordnaren samt eventuellt sakkunniga för respektive behandling.
- Förbered utbildningsinsatsen med förberedande halvdagsworkshop där DSO med informationssäkerhetssamordnaren från respektive förvaltning av de sex fackförvaltningarna som delar DSO, skapar samsyn inte minst för processen att sammanställa information för registerförteckning, informationsklassning, riskanalys och eventuell konsekvensbedömning.

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.

Stadens obligatoriska rapporteringsområden är

- registerförteckning,
- styrdokument samt fastställda rutiner och processer
- tekniska och organisatoriska säkerhetsåtgärder för personuppgiftsbehandlingar,
- konsekvensbedömningar,
- individens rättigheter och
- personuppgiftsincidenter.
- Personuppgiftsbiträdesavtal med instruktioner

I rapporten redogörs för bedömning av bolagets status på efterlevnaden av kontrollerade rapporteringsområden, samt DSO:ns slutsatser samt rekommendationer för förbättringsinsatser.

Dataskyddsförordningen pekar genomgående på att arbetssätt och rutiner *skall* vara dokumenterade. Detta kan sättas i relevans till kravet på att den personuppgiftsansvarige måste kunna *visa* att Dataskyddsförordningen principer för behandling av personuppgifter efterlevs (artikel 5).

3.1 Registerförteckning

3.1.1 Bakgrund och syfte

Förteckning på behandlingar, även kallad registerförteckning, är viktigt på flera punkter. Det är lagkravkrav på att kartlägga de behandlingar som görs på personuppgifter samt att dokumentera kartläggningen med ett antal informationsuppgifter kravställda att de skall ingå som minimum i dokumentationen. Dessutom är förteckningens ingående information viktigt för att kunna arbeta med dataskydd, registerförteckningen kan sägas vara såväl grunden för och centralt för arbetet med att efterleva Dataskyddsförordningen.

Dataskyddsarbetet bör ha initierats av kartläggning och dokumentation på behandlingarna där minst villkorade informationspunkter kan ingå. Till det finns det informationspunkter som, i det fall de ingår, underlättar kontroll- och förbättringsarbetet.

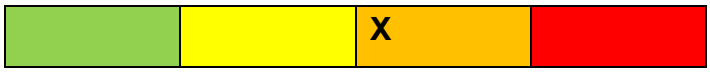
Dokumentationen är det som benämns som Registerförteckningen, som skall hållas uppdaterad i vart fall på årsbasis eller då förändringar sker som förändringar i befintliga behandlingar, nya behandlingar eller behandlingar som upphört.

Syftet med kontroll av registerförteckningen är för att stämma av att den hålls uppdaterad, aktuell och komplett. Om brister noteras av DSO så rekommenderar denne lämpliga förbättringsinsatser.

3.1.2 Resultat

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	93
Har nödvändiga uppdateringar gjorts?	Omfattande brister för inlagd information
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Oklart, dokumentation av rutinerna förordas
Övrigt	Tröskelanalys kan vara alternativ till konsekvensbedömning

3.1.3 Status för brister gällande registerförteckningen



Under året har överföring av registerförteckningen skett, vilket inneburit ett omfattande arbete. Det fortsatta arbetet med att komplettera registerförteckningen är planerat. Vissa delar av informationen finns men behöver sammanställas. Andra delar av informationsinsamlande är beroende av tidsavsättning från informationsägare, och kräver ett annat angreppssätt.

Bristerna i registerförteckningen är 77 % i medelvärde, och är upp till 100 % för flera av de viktigaste informationspunkterna.

Tröskelanalysgenomförande fortsätter nästa år. Specificerat om konsekvensbedömning resp Tröskelanalys under avsnitt ”Tekniska och organisatoriska säkerhetsåtgärder”.

3.1.4 Rekommendationer till PUA

- Säkerställa att förvaltningen har nödvändiga resurser
- Ett tydligt fokus för 2023 bör vara att komplettera informationen i registerförteckningen
- Införa årsmässig genomgång av registerförteckningen, ansvar på informationsägare.

- Införa stöd i form av utökat samarbete dels mellan extern DSO och respektive centrala roller för varje fackförvaltning för att dela samsyn och information mellan rollerna.
- Även införa stöd i form av utökat samarbete samt mellan de sex fackförvaltningarna för att hitta en större samsyn kring dataskyddsarbetet mellan förvaltningarna som delar extern DSO.
- Information om informationsklassning riskanalys och konsekvensbedömning är särskilt låg, där 100 % saknas. Hög prioritet för komplettering rekommenderas. Även viktig information som säkerhetsåtgärder ligger på höga bristvärden.

3.2 Styrdokument

3.2.1 Bakgrund och syfte

I detta avsnitt avses till att börja med de styrande dokument som uttrycker ledningens vilja i dataskyddsarbetet. Dokumentationen beskriver roller som har ett ansvar att upprätthålla efterlevnaden av Dataskyddsförordningen. Förslagsvis tjänsteägare och liknande roller, registrator, kundtjänst och projektledare.

Dessutom kontrolleras i detta avsnitt dokumentation som beskriver hantering av personuppgiftsincidenter samt beskrivning av hantering av registrerades rättigheter. Antalet registrerade incidenter, inkomna begäran om rättigheter samt dessa processer, hanteras i egna avsnitt. I detta avsnitt kontrolleras existensen av dokumentation, deras kvalitet och spårbarhet.

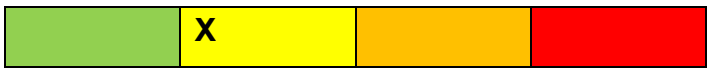
Genom styrdokument kommunicerar PUA till medarbetare i sin verksamhet om vad som gäller och vad som förväntas av medarbetarna, när de hanterar personuppgifter. Att styrdokument finns nedtecknade, beslutade och kommunicerade medför att medarbetaren får information om regler, ramar och förutsättningar och stöd för att behålla kunskapen över tid och tillämpa den på ett konsekvent sätt.

3.2.2 Resultat

Fråga/kontroll	Svar
Är dokumenten av lämpligt format, är pedagogiska och ger tillräckligt stöd?	Ja
Är dokumenten uppdaterade?	Framgår inte i alla dokument
Finns informationsägare till dokumenten, så att ansvar för uppdateringar är tydliga?	Framgår inte i alla dokument

Ange dokumenten med namn och deras syfte, detta ger en kontroll på vilka dokument man hänvisar till.	1)Roll och ansvarsbeskrivning: 2)Vägledning för hantering av PU incident: ”PU incident process beskrivning” samt ”Vägledning för personuppgiftincidenthantering” 3)Rutin för registrerades rättigheter: ”Blankettbegäran om registerutdrag enligt artikel 15 Dataskyddsförordningen” samt ”Rutin för handläggning av begäran om registerutdrag avseende personuppgifter”

3.2.3 Status för brister gällande styrdokument



Alla nödvändiga dokument finns, önskvärda förbättringar är att fastställa interna informationsägare för dokumenten, och att ha en post så att senaste uppdatering framgår i tid.

3.2.4 Rekommendationer till PUA

- Stötta organisationen att göra rekommenderade förbättringsinsatser gällande styrdokument så att en fastställd informationsägare finns för varje dokument och ett fält där datum för senaste uppdatering framgår.

3. Tekniska och organisatoriska säkerhetsåtgärder

3.2.6 Sammanfattning och syfte

Tekniska och organisatoriska säkerhetsåtgärder krav ställer att informationssäkerhet är en del av organisationens arbete, och dataskyddsarbetet villkoras av detta arbete.
Syftet med att granskningen är att säkerställa säkerhetsresurser för respektive behandling.

GDPR krav på tekniska respektive organisatoriska säkerhetsåtgärder motsvaras som regel av fungerande och komplett IT-säkerhet och reglerad och fastställd åtkomst i form av roller med definierad access och rättigheter både fysiskt i lokaler och till system, andra digitala resurser samt den *organisatoriska* strukturen.

Organisatoriska säkerhetsåtgärder innebär till stor del det systematiska arbetet som innebär med registerförteckning/kartläggning inklusive nedanstående aktiviteter, som skall dokumenteras på ett konsekvent sätt

- Informationsklassning av personuppgifterna
- Riskanalys
- Tröskelanalys som fastställer om konsekvensanalys behöver göras
- Eventuell konsekvensanalys

3.2.7 Resultat

Fråga/kontroll	Svar
Är alla behandlingar med personuppgifter informationsklassade? Om inte hur många är ej klassade?	Information saknas i registerförteckningen. Enligt uppgift skall klassning vara gjord för alla utom två.
Är klassningarna aktuella? Om brister, hur många?	Inga kontroller av aktualitet av klassningar har gjorts under året.
Är behandlingarna riskanalyserade, om brist ange hur många?	Uppgifterna saknas för alla
Finns tröskelanalys för alla behandlingar, alternativt konsekvensbedömning? Om inte, hur många saknas?	Konsekvensbedömning för alla behandlingar. (Tröskelanalys är ej införd ännu.)
Finns tekniska säkerhetsåtgärder som följer Stadens riktlinjer för alla behandlingar?	Saknas för 73 av 93
Finns organisatoriska säkerhetsåtgärder	Saknas för alla utom 1

3.2.8 Status för brister tekniska och organisatoriska säkerhetsåtgärder

- Klassningar och riskanalyser har gjorts i stor omfattning, men behöver kontrolleras under kommande år samt föras in i registerförteckningen
- Uppgifter som informationsklassning, riskanalys behövs för att göra tröskelanalys, tröskelanalys kan användas för att bedöma om konsekvensbedömning behövs eller inte. Om konsekvensbedömning bedöms behöva göras, så utgör informationen från informationsklassning, risk- och tröskelanalys tillsammans med övrig information om behandlingen i registerförteckningen underlag för konsekvensanalys.

3.2.9 Rekommendationer till PUA

Tillse att verksamheten har medel och resurser för att arbeta med:

- Informationsägare skall ha tydliga direktiv för prioritering och att avsätta tid för arbete med informationsklassning, riskanalys samt ansvara för lämpliga organisatoriska säkerhetsåtgärder
- Införa stöd i form av utökat samarbete dels mellan extern DSO och respektive centrala roller för varje fackförvaltning för att dela samsyn och information mellan rollerna.
- Även införa stöd i form av utökat samarbete samt mellan de sex fackförvaltningarna för att hitta en större samsyn kring dataskyddsarbetet mellan förvaltningarna som delar extern DSO.
- Information om informationsklassning riskanalys och konsekvensbedömning är särskilt låg, 100 % saknas. Hög prioritet rekommenderas.

3.3 Konsekvensbedömningar

3.3.1 Sammanfattning och syfte

Behandlingar som kan innebära risker av en viss nivå skall enligt Dataskyddsförordningen bedömas utifrån vilka potentiella negativa konsekvenser behandlingen kan innebära för de behandlade.

Därför behöver varje behandling genomgå en tröskelanalys som värderar vad som framkommit vid kartläggning/registerförteckning av behandlingen, riskbedömning av ingående personuppgifter samt riskanalysen.

Om tröskelanalysen ger att konsekvensbedömning inte behöver göras skall denna bedömning dokumenteras och lagras i anslutning till behandlingen så att spårbarhet finns. Stöd för att göra detta arbete konstruktivt och med rätt kvalitet behöver finnas.

Syftet med kontroll av konsekvensbedömning består av två delar, dels om antingen tröskelanalys eller konsekvensbedömning har gjorts för varje behandling, dels att stöd för dessa rutiner finns, är kända och används.

3.3.2 Resultat

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Nej

Har alla potentiella högriskbehandlingar konsekvensbedömts?	Nej
Är de genomförda bedömningarna aktuella?	Ej aktuellt då brist är 100 %
Har tröskelanalys, med dokumentation, gjorts för alla behandlingar som inte är konsekvensbedömda?	Information om konsekvensbedömning saknas till 100 %. Tröskelanalys har diskuterats att införas i arbetsprocessen
Finns relevant stöd, som instruktioner, mallar och utbildning, för detta arbete?	Mall för konsekvensbedömning finns: Mall konsekvensbedömning DPIA - v 1 1 2022-05-11

3.3.3 Status för brister gällande konsekvensbedömningar

Den underliggande informationen för att kunna avgöra om konsekvensanalys behövs, och för att genomföra konsekvensanalysen saknas genomgående för behandlingarna.

Därför rekommenderas en justering på arbetsmodell, som har presenterats för administrativa chefer och som är planerad Q1 2023. Dessförinnan bör DSO haft samrådande kring detta med informationssäkerhetssamordnaren.
Arbetsmodellen inkluderar att systematiskt arbeta sig genom registerförteckning, informationsklassning samt riskanalys för att dessa faktorer skall utgöra underliggande information att bygga behov och eventuellt genomförande av konsekvensanalys.

Ett tydliggörande till de roller som innehar informationsägarskapet är också en viktig del i ett framgångsrikt arbete. Mer om det under avsnitt ”Övrigt att rapportera”.

3.3.4 Rekommendationer till PUA

- Tillse att verksamheten har medel och resurser för att förändra arbetssätt och arbeta med dataskyddsarbetet strukturerat och kontinuerligt
- Informationsägare skall ha tydliga direktiv för prioritering och att avsätta tid för arbete med tröskelanalys och konsekvensbedömning då det behövs.
- Införa stöd i form av utökat samarbete dels mellan extern DSO och respektive centrala roller för varje fackförvaltning för att dela samsyn och information mellan rollerna.
- Även införa stöd i form av utökat samarbete samt mellan de sex fackförvaltningarna för att hitta en större samsyn kring dataskyddsarbetet mellan förvaltningarna som delar extern DSO.

3.4 Individens rättigheter

3.4.1 Sammanfattning och syfte

Individens rättigheter innefattar flera krav i Dataskyddsförordningen. Registrerade har rätt att begära och få registerutdrag. De har också rätt att exempelvis begära att bli raderade och få sina uppgifter rättade. I båda dessa fall kan det vara svårt att möta begäran, dels för att exempelvis radering kan gå i strid med det uppdrag som personuppgiftsansvarig är skyldig att utföra, för rättningsbegäran kan detta vara svårt att möta eftersom de personuppgifter som behandlas kommer från annan part.

Kontroll av individens rättigheter görs för att kontrollera att de interna rutinerna fyller sitt syfte och är effektiva.

3.4.2 Resultat

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	1
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	1

3.4.3 Status för brister gällande individens rättigheter

X			

- Ingen brist har noterats

3.4.4 Rekommendationer till PUA

- Ingen brist har noterats

3.5 Personuppgiftsincidenter

3.5.1 Sammanfattning och syfte

Identifiera och hantera personuppgiftsincidenter är viktiga av flera anledningar, dels är det krav i Dataskyddsförordningen, men det ger även verksamheten möjlighet att identifiera brister i dataskyddet och införa åtgärder.

Kontrollområdet säkerställer både att det finns en medvetenhet som gör att personuppgifts-incidenter upptäcks och att det finns en fungerande process att hantera personuppgiftsincidenter. Samt kontrollerar att det planeras och utförs åtgärder för de brister som personuppgiftsincidenten identifierat.

3.5.2 Resultat

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	I detta fall av biträdet
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?	-

Med utgångspunkt för den inträffade incidenten fungerar handläggande på Idrottsförvaltningen väl.

Idrottsförvaltningen har en vägledning för hantering av personuppgiftsincident. I vägledningen saknas information om vilka roller som bör ingå i analys och beslutsprocessen. Som exempel kan man välja att närmaste chef dokumenterar den misstänkta personuppgiftsincidenten och konsulterar vid osäkerhet huruvida det är en personuppgiftsincident eller ej, samt osäkerhet om den skall rapporteras till IMY.

Ett kompletterande stöd skulle kunna vara en mall för att fylla i de uppgifter som gör att bedömning kan göras, underlaget kan sedan användas för eventuella samråd med DSO och arkiveras med beslut.

Ytterligare en notering är att det låga antalet rapporterade misstänkta personuppgiftsincidenter *kan* bero på en underrapportering. Exempelvis på grund av osäkerhet kring vem som ansvarar för att rapportera en misstänkt personuppgiftsincident.

3.5.3 Status för brister gällande personuppgiftsincidenter

Det förefaller vara ett par brister för personuppgiftsincidenthanteringen:

- Det framgår ej av vägledning vilka personer som äger ansvaret för att lyfta personuppgiftsincidenten och vart man lyfter.
- Ett bra stöd är en mall som efterfrågar den information som ger bra bedömningsunderlag.

3.5.4 Rekommendationer till PUA

- Tilldela Idrottsförvaltningen medel för att införa förbättrande åtgärder för personuppgiftsincidenthantering,
- Definiera och införa organisation för hantering av misstänkta personuppgiftsincidenter
- Ta fram och införa ett mallstöd för att sammanställa information för bedömningsunderlag, samt dokumentation av beslut.

3.6 Personuppgiftsbiträdesavtal

3.6.1 Sammanfattning och syfte

För varje personuppgiftsbehandling skall personuppgiftsbiträdesavtal PuB avtal finnas i det fall ett biträde (leverantör) används. Behandlingarna skall beskrivas och regleras i enlighet med Stadens framtagna mall för PuB avtal. Personuppgiftsbiträdesavtalens riktighet bör kontrolleras med bestämd frekvens,

Post för att ange då för PuB-avtal behövs finns med i registerförteckningen, likaså post för att ange rutiner för att PuB avtalens riktighet följs upp.

3.6.2 Resultat

Fråga/kontroll	Svar
Är behovet av PuB avtal definierat för alla behandlingar	Nej information saknas för 91 av 93 behandlingar
Finns rutiner för uppföljning av PuB avtal	Nej saknas för 92 av 93 behandlingar

Observera att avsaknaden av information inte nödvändigtvis innebär att PuB avtal saknas i de fall där det behövs. Här saknas dock information om eventuellt behovet av PuB avtal är klarlagt. Då PuB avtal finns bör rutiner för uppdatering finnas för att kontinuerligt och systematiskt arbete skall råda.

3.6.3 Status för brister gällande personuppgiftsbiträdesavtal

Information finns till stora delar. Dock behöver inventering av befintliga PuB avtal göras, och framtagning av motivering då PuB avtal inte behövs. Samt dokumentation av detta i registerförteckning.

3.6.4 Rekommendationer till PUA

Ge Idrottsförvaltningen resurser för

- systematisk och kontinuerligt dataskyddsarbete skall kunna utföras, som fastställande av behovet eventuellt PuB avtal.

4 Strategi för granskningar

4.1 Det gångna årets granskningar

Granskningarna genomförts under en period i slutet av året, genom analys av informationen i registerförteckningen, samt informationsinsamling från nyckelroll.

4.2 Planerade granskningar kommande år

Exempelvis skulle man kunna ha en definierad arbetsgrupp som har en gemensam planering inför arbetet med GDPR årsrapport. Det skulle kunna ge att man i samsyn planerar för aktiviteter under året för förbättringsåtgärder, samlar relevant information kontinuerligt samt i god tid uppdaterar registerförteckningen. Detta skulle kunna innebära att sammanställningen av GDPR årsrapport sker på kort tid och resultatet av granskningen kan då internt det kunna vara samsyn kring.

5 Övrigt att rapportera

5.1 Sammanfattning och syfte

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

5.2 Observationer utöver granskningsområden

Observation 1

Dataskyddsarbetet är beroende av flera roller där rollen informationssäkerhetssamordnaren är central för att hålla ihop arbetet med informationsklassning och riskanalys, medan objektansvarig ansvarar för behandlingen som har information om själva behandlingen och vilka personuppgifter som ingår.

Risk: Om inte samsyn kring ansvar och ägarskap upprättas kring dessa moment inom dataskyddsarbetet kan det innebära att det är svårt att höja kvalitén på dataskyddarbetet.

Observation 2

Under hösten har administrativ chef beställt kompletterande utbildning för de roller som behöver förstå Dataskyddsdelarna i sitt eget ansvarsområde.
Utbildningen är planerad att genomföras under Q1 2023.

Observation 1			X	
Observation 2	X			

5.3 DSO rekommendationer till PUA

- Förutsättningar för nära samarbete mellan DSO, informationssäkerhetssamordnaren samt eventuellt sakkunniga för respektive behandling.
- Förbered utbildningsinsatsen med förberedande halvdagsworkshop där DSO med informationssäkerhetssamordnaren från respektive förvaltning av de sex fackförvaltningarna som delar DSO, skapar samsyn inte minst för processen att sammanställa information för registerförteckning, informationsklassning, riskanalys och eventuell konsekvensbedömning.