Stockholms stad

Bilaga 5

GDPR Årsrapport

2021

Idrottsnämnden

GDPR årsrapport
December 2021

Utgivningsdatum: 2021-12-28
Kontaktperson: Carina Braun

1 Bakgrund

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

Enligt dataskyddsförordningen är varje nämnd och bolagsstyrelse inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnd och bolagsstyrelse behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett dataskyddsombud, DSO. DSO har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är således ett medel för nämnd och styrelse att ta emot de råd och rekommendationer som dataskyddsombudet är skyldig att ge till ansvarig enligt dataskyddsförordningen, samt för nämnden att få insyn i vad DSO:s granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnd ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnd eller bolagsstyrelse ska kunna *visa* att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna *dokumenteringsskyldighe*t. Årsrapporten är även ett medel för nämnds uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehåll

2 Sammanfattning

I egenskap av ert dataskyddsombud lämnar jag följande årsrapport.

År 2021 har ordinarie dataskyddsombud varit föräldraledig och rollen har övertagits av närmaste chef Carina Braun.

Informationssäkerhet- och dataskyddsarbetet inom idrottsförvaltningen sker med hjälp av en arbetsgrupp med flera nyckelfunktioner.

Under det gångna året har fokus legat på individens rättigheter, det vill säga att det ska finnas tydliga rutiner för registerutdrag, en översikt av de allmänna villkoren för entré till stadens simhallar med mera. En granskning av processen för arbetet med organisationens registerförteckning och utformningen av själva dokumentet har skett. Vid nedtecknandet av denna rapport framkommer att flera rutiner finns på plats och tillämpas ad hoc i organisationen, men de är inte dokumenterade och kommunicerade.

Det hela kan sammanfattas i följande punkter:

- Ombesörja att rutiner som identifierats att behöva dokumenteras och kommuniceras sker under 2022.
- Fortsätta att utbilda samtlig personal i dataskyddsförordningen
- Utse ansvariga för respektive personuppgiftsbehandlingar
- Utse ansvariga för rutiner så att dessa kan hållas uppdaterade

3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som personuppgiftsansvarig, PUA, som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som dataskyddsförordningen avser.

De obligatoriska rapporteringsområdena är registerförteckning, styrdokument, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, konsekvensbedömningar, individens rättigheter och personuppgiftsincidenter.

Nedan redogörs för nämndens eller bolagets status och DSO:s slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:s genomförda uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	72 st
Har nödvändiga uppdateringar gjorts?	Till viss del
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Till viss del

3.1.2 Syfte

För att något ska gå att skydda måste det först vara synligt för verksamheten. Det följer därför i klartext av dataskydds-förordningen (artikel 30) att stadens alla förvaltningar och bolag måste inventera alla personuppgifter som behandlas i verksamheten, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde, och dokumentera dem i en så kallad registerförteckning (även kallat behandlingsregister).

När registerförteckningen är upprättad skapar den en intern synlighet och förståelse för vilka personuppgifter som behandlas samt hur de hanteras. Registerförteckningen är därför dataskyddsarbetets centrala utgångspunkt och bas samt säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling. Det är därför viktigt att PUA får information om hur komplett verksamhetens förteckning är. Om dokumenteringskravet uppfylls kan verksamheten arbeta effektivt, systematiskt och riskbaserat och samtidigt värna individens integritet, särskilt när känsliga och särskilt skyddsvärda personuppgifter behandlas av verksamheten.

Att ha en registerförteckning på plats leder till att verksamheten kan arbeta mer resurs- och kostnadseffektivt med sitt systematiska och riskbaserade dataskyddsarbete. Man kan styra insatserna där de gör störst nytta.

Syftet med detta rapporteringsområde är således att rapportera till PUA hur väl verksamheten har lyckats inventera sina personuppgifter och de personuppgifter som behandlas för annans räkning och upprätta en registerförteckning.

Eftersom inventeringen av personuppgifter i sig är avgörande för allt det fortsatta dataskyddsarbetet inom verksamheten, är denna lägesbild en av de viktigaste slutsatserna som PUA behöver förstå och ta ställning till inför det planerade åtgärdsarbetet under nästa verksamhetsår.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

72 behandlingar.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Uppdateringar är inte fullständiga. Arbete pågår med att uppdatera förteckningen. I samband med uppdateringen ska förteckningen flyttas och bli en del av förvaltningens hanteringsanvisning.

DSO bedömer hur fullständig registerförteckningen är

Registerförteckningen är i ett grundutförande men är inte fullständig. Kravbilden har förändrats sedan 2018 när lagstiftningen infördes.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Till viss del då processer och rutiner finns, men är inte dokumenterade, beslutade och kommunicerade.

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

Idag sker arbetet med registerförteckningen efter odokumenterade rutiner.

3.1.5 DSO ger råd och rekommendationer till PUA

Dokumentera och kommunicera rutin för registerförteckning. Arbetet kan med fördel utföras i dataskydd och informationssäkerhetsgruppen.

Organisationen behöver fortsätta med uppdatering av registerförteckningen i syfte att kvalitetssäkra personuppgiftsbehandlingarna. En anpassning mot ny kravbild ska genomföras samt kompletteras med eventuella personuppgiftsbehandlingar som kan ha tillkommit.

Arbete med att nuvarande registerförteckning ska integreras i förvaltningens hanteringsanvisning i syfte att effektivisera och kvalitetssäkra hanteringen av personuppgifter. Registrator, nämndsekreterare, informationssäkerhetssamordnare och systemadministratör säkerhet ansvarar för att genomföra integreringen under 2022.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Till viss del
Håller innehållet i de existerande dokumenten lämplig kvalitet?	JA
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	JA
Är dokumenten uppdaterade?	JA
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	JA

3.2.2 Syfte

Området syftar till att PUA genom styrdokument ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. 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 dataskyddsinformation och kan behålla kunskapen över tid och tillämpa den på ett konsekvent sätt. En röd tråd i dataskyddsförordningen är att viktiga arbetssätt och rutiner ska vara dokumenterade. Detta följer bland annat av kravet på att den personuppgiftsansvarige måste kunna *visa* att dataskyddsförordningens principer för behandling av personuppgifter efterlevs (artikel 5).

Rapporteringen av området är tvådelad: dels ska DSO bedöma om verksamheten har styrdokument antagna och på plats, dels ska rapporteringen visa om dokumentationen innehållsmässigt håller en lämplig kvalitet, i vilket ingår bland annat att dokumentationen ska vara uppdaterad och aktuell.

En brist inom detta område bör förstås 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 exempelvis ofta till *bristande kvalitet* i hur verksamheten utför aktiviteterna, men även till att verksamheten *slösar värdefulla resurser* när exempelvis för många personer blir involverade i en incidenthantering eller för att en analys behöver göras om från grunden varje gång istället för att man återanvänder redan uppfunnen kunskap. Dessa effekter drabbar verksamheter ur ett vidare perspektiv och är något som ligger i PUA:s intresse att förstå för att fatta rätt beslut om.

Eftersom flera av styrdokumenten omfattar både dataskydd och informationssäkerhet bör DSO resonera med informationssäkerhetssamordnare i bedömningar och förslag på åtgärder framåt för nästa verksamhetsår.

3.2.3 Resultat

Centrala riktlinjer finns och följs för hur verksamheten hanterar säkerhetsåtgärder för personuppgiftsbehandling och rutin för uppföljning och revidering av behörigheter. Dessa är publicerade på Stockholms stads intranät. En lokal rutin och blankett finns för begäran om registerutdrag samt en rutin för hur e-posthantering ska ske inom organisationen. Ansvariga för rutinerna är chef för administrativa avdelningen och IT-chef. Utbildning genomförs löpande och regelverk kommuniceras.

Brister är identifierade inom följande områden:

- Lokal rutin för hantering av personuppgiftsincidenter saknas.
- Lokal rutin för konsekvensbedömning saknas.
- Lokal rutin för sociala media saknas.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

Ja

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
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

Då det saknas lokal rutin för personuppgiftsincidenthantering är detta orsaken att bristen anses som mer allvarlig.

3.2.5 DSO ger råd och rekommendationer till PUA

- Rutin för hur personuppgiftsincidenter ska hanteras ska tas fram. Kan med fördel göras i samarbete med rutin för informationssäkerhetsincidenter.
- Rutin för konsekvensbedömning ska tas fram
- Rutin för sociala media ska 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?	16
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Utan informationsklassningen har verksamheten inte förutsättningar att välja rätt åtgärder för att skydda sin information. Det är därför av stor betydelse för dataskyddsarbetet att PUA ges en uppdaterad bild varje år av huruvida informationsklassning är genomförd för personuppgifter som verksamheten hanterar.

Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare. En första kontrollpunkt måste därför vara om en informationsägare eller en informationsägarrepresentant med ansvar för klassning är identifierad i verksamheten. Om en ansvarig för klassningen inte har pekats ut och känner till sitt ansvar för klassning, minskar sannolikheten avsevärt att en klassning faktiskt initieras.

Notera att enbart sådan informationsklassning som avser behandling eller system som omfattar *personuppgifter* är av intresse för DSO:s årsrapportering.

Eftersom informationsklassning är ett arbete som görs inom ramen för informationssäkerhetsarbetet, bör DSO samråda och planera uppföljningen tillsammans med informationssäkerhetssamordnare. Enligt stadens metodik klassas personuppgifter och övrig information i samma workshop, och slutsatserna kring klassningen dokumenteras i samma protokoll.

Viktigt är också att notera att dataskyddsombudet omhändertar den registrerades intresse och informationssäkerhetssamordnaren har fokus på verksamhetens krav på informationen i form av tillgänglighet, riktighet och konfidentialitet. Verktyget för DSO är i första hand registerförteckningen och dokumentationen där. Informationssäkerhetssamordnaren har KLASSA som verktyg för att se till att verksamhetens krav efterlevs i form av dokumentation i förvaltningsplaner, systembeskrivningar etc.

3.3.3 Resultat

KLASSA har genomförts för 16 stycken system som innefattar personuppgiftsbehandlingar.

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

Registerförteckningen innehåller inte informationsklassning.

3.3.5 DSO ger råd och rekommendationer till PUA

Organisationen behöver uppdatera registerförteckningen med de tekniska och organisatoriska åtgärder som vidtagits för respektive personuppgiftsbehandling.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

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?	-

3.4.2 Syfte

Konsekvensbedömningen hjälper en organisation att identifiera och minimera integritetsriskerna för personuppgifter som behandlas i projekt eller linjeverksamhet. En konsekvensbedömning har till syfte att identifiera och dokumentera risker kopplade till en viss behandling, samt att bedöma sannolikheten och konsekvensen om riskscenariot skulle inträffa. Baserat på bedömningen kan/ska riskförebyggande åtgärder vidtas.

Konsekvensbedömningen anses liksom registerförteckning och informationsklassning som ett viktigt verktyg för verksamhetens dataskyddsarbete. Kravet på konsekvensbedömning är dessutom ett uttryckligt krav enligt dataskyddsförordningen och ska utföras för alla behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1). Notera att Integritetsskyddsmyndigheten (IMY) på sin webbplats har publicerat en förtydligande förteckning över när personuppgiftsbehandlingar kräver en konsekvensbedömning. Det är viktigt att PUA genom årsrapporten får en uppdaterad bild av hur fullständig verksamhetens situation är i fråga om konsekvensbedömningar avseende dataskydd.

3.4.3 Resultat

Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?

Nej

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Nej

Är de genomförda konsekvensbedömningarna 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
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

Organisationen saknar skriftlig rutin för konsekvensbedömningar.

3.4.5 DSO ger råd och rekommendationer till PUA

Organisationen har flera personuppgiftsbehandlingar som behöver dokumenteras i konsekvensbedömningar. Ett exempel på detta är kameraövervakning. Syftet är att organisationen kan se att den efterlever samtliga identifierade risker och påföljande krav som finns, samt visa hur och varför val har gjorts i tekniska och organisatoriska lösningar.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	Kan ej anges då endast nekande diarieförs enligt SSA 2016:01 Hanteringsanvisning 2.4.2 och 2.8
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	Samtliga då inga avvikelser framkommit

3.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen (artikel 12–22) ett antal rättigheter som på olika sätt ska garantera att den registrerade personen har insyn i hur dennes personuppgifter hanteras samt har en viss kontroll över personuppgiftsbehandlingen. Det är ett krav enligt förordningen att den verksamhet som enligt förordningen är att se som personuppgiftsansvarig – det vill säga i stadens fall nämnder och bolag – tillgodoser rättigheterna i fråga.

Rättigheterna medför en rätt att ställa krav på att verksamheten vidtar vissa åtgärder, som exempelvis att lämna ut ett så kallat registerutdrag eller att rätta vissa uppgifter. (Radering, den så kallade ”rätten att bli glömd”, är sällan aktuell i någon större mån eftersom stadens verksamheter lyder under krav på bevarande till följd av offentlighetsprincipen.) Verksamheten har enligt dataskyddsförordningen artikel 12.3 en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran. (Notera dock att det finns undantagssituationer angivna i artikel 12.3, där fristen kan förlängas till mer än en månad.)

Dataskyddombudet har en roll i att granska efterlevnaden, identifiera brister samt ge råd och stöd i hur processer och rutiner för att tillgodose rättigheterna bör utformas.

Om verksamheten inte klarar av att hantera en begäran från en registrerad person i enlighet med dataskyddsförordningens krav, kan det skada allmänhetens förtroende för hur staden hanterar personuppgifter. Det kan även leda till tillsynsärenden från Integritetsskyddsmyndigheten (IMY), med sanktioner som följd. Det är därför viktigt att PUA regelbundet ges en bild av i vilken mån verksamheten klarar av att leva upp till regelverkets krav på att hantera begäran inom föreskriven tidsfrist.

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

Ja

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

Registraturet har en befintlig process och skriftlig rutin för hur detta ska hanteras.

3.5.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudets råd är att kommunicera detta under år 2022 till samtlig personal.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Internt av medarbetare inom förvaltningen samt information från stadsledningskontoret.
Hur många personuppgiftsincidenter har dokumenterats?	1 – centralt system inom staden
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?	-

3.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskyddsförordningen (artikel 4.12) ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.”

I en verksamhet kan det förekomma många andra typer av incidenter, som inte involverar personuppgifter. Det är viktigt att hålla den saken i åtanke, så att årsrapporteringen inte omfattar annat än just personuppgiftsincidenter. Vidare är det en grundförutsättning för hanteringen av personuppgifter att incidenter över huvud taget upptäcks, samt att verksamheten förstår att hantera incidenter som rör personuppgifter på det särskilda sätt som dataskyddsförordningen kräver.

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland dataskyddsförordningens olika verktyg för att åstadkomma en sund personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering. Stadens mall för DSO:s årsrapport är avsedd att fokusera på rapporteringen.

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag från rapporteringsskyldigheten gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” (se artikel 33). Detta innebär att de flesta personuppgiftsincidenter ska rapporteras till IMY, inte senare än 72 timmar efter att verksamheten fått vetskap om incidenten. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter och friheter, ska rapportering även ske till de berörda registrerade personerna, utan dröjsmål. Dataskyddsförordningen delar alltså in personuppgiftsincidenter i tre kategorier: ingen rapportering, rapportering till IMY samt rapportering till de berörda personerna.

Bristande förmåga att rapportera personuppgiftsincidenter i tid kan leda till sanktioner från IMY. DSO:s årsrapportering är därför avsedd att kartlägga detta, samtidigt som det finns möjlighet att redovisa vilka typer av personuppgiftsincidenter som inträffat, incidenternas allvarsgrad etc.

Notera att enligt dataskyddsförordningen artikel 33.5 ska alla personuppgiftsincidenter dokumenteras, det vill säga även i de fall då incidenten inte ska rapporteras till IMY. Bristande dokumentering står i strid med Dataskyddsförordningen och leder även till problem med att ta fram korrekta siffror till årsrapporteringen avseende hur väl verksamheten lever upp till rapporteringsfristerna. Enligt artikel 33.5 är det ett krav att dokumentera omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden och bristande dokumentering är sanktionsgrundande.

3.6.3 Resultat

Organisationen har inte haft några egna rapporterade personuppgiftsincidenter under 2021.

3.6.4 DSO anger hur allvarliga bristerna är på en skala

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

Organisationen saknar skriftlig rutin för hantering av personuppgiftsincidenter.

3.6.5 DSO ger råd och rekommendationer till PUA

Avsaknaden av personuppgiftsincidenter kan vara en indikator att kunskapen om detta är låg. Detta kan vara ett resultat av att rutinen för personuppgiftsincidenter inte är framtagen, implementerad och kommunicerad.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Granskning av registerförteckningen
- Granskning av rutin för registerutdrag

4.2 Syfte

En av dataskyddsombudets 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

Granskning av 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

Granskat rutin för 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
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	Inga brister av nämnvärd betydelse identifierade

4.4 DSO ger råd och rekommendationer till PUA

Se kapitel registerförteckning

Se kapitel individens rättigheter

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- Bristande rutiner och handläggning inom dataskydd

5.2 Resultatet av riskkartläggningen

Risk 1 - Bristande rutiner och handläggning

	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

5.3 DSO ger råd och rekommendationer till PUA

Fortsätta säkerställa kunskapsnivån inom förvaltningen. Sakkunniga deltar fortlöpande i utbildningar. Informationssäkerhet- och data-skyddsgruppen identifierar och hanterar utvecklingsbehov samt eventuella brister.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Dataskyddsombudet ska under 2022 granska följande områden:

- Granska att skriftliga rutiner har tagits fram där det saknas.
- Granska att dataskyddsfrågan omhändertas i arbetet med informationssäkerhetsverktyget KLASSA.

6.2 Syfte

En av dataskyddsombudets 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 personuppgiftsansvarig är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under det gångna året och vad resultaten av granskningarna är.

6.3 Planerade granskningar

- Granska att skriftliga rutiner har tagits fram där det saknas.
- Granska att dataskyddsfrågan omhändertas i arbetet med informationssäkerhetsverktyget KLASSA.

7 Övrigt att rapportera

7.1 Syfte

Avsikten med denna punkt i årsrapporten är att ge möjlighet att komplettera bilden av statusen i dataskyddsarbetet. Under denna rubrik anges sådant som inte på ett naturligt sätt tas upp under någon av punkterna i rapporteringsstrukturen ovan, eller som inte heller ryms i den inledande sammanfattningen.

7.2 Övriga observationer

Observation 1

Under 2021 har en person inkommit med klagomål till Integritetsskyddsmyndigheten, IMY, mot idrottsförvaltningen. IMY kontaktade förvaltningen för att informera om klagomålet. Organisationen hade redan vidtagit flera åtgärder efter att den upplysts av den klagande vilket visar på en god lyhördhet när problem uppstår och en vilja att förbättra och förändra när behov uppstår.

Observation 2

Upphandlare har arbetat aktivt under året med att få in personuppgiftsbehandling som en fråga vid upphandlingar. Detta för att underlätta tecknande av personuppgiftsbiträdesavtal.

7.3 DSO ger råd och rekommendationer till PUA

Det goda exemplet med arbetet inom upphandling och personuppgiftsbiträdesavtal är bra om det kommuniceras till organisationen. Detta för att inspirera till egna initiativ i arbetet med dataskyddsförordningen.