



Stockholms  
stad

# GDPR Årsrapport

År 2024

Idrottsnämnden

**GDPR årsrapport 2024**

December 2024

**Dnr:** YYYY

**Utgivningsdatum:** 2025-01-10

**Kontaktperson:** Christian Sandell

# 1. Bakgrund

Dataskyddsförordningen (nedan GDPR) trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen är 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. GDPR syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna inom EU.

Även om Stockholms stad (nedan Staden) är en juridisk person har Kommunstyrelsen uttalat att vare nämnd inom Stockholms stad ska anses vara personuppgiftsansvarig för de personuppgifter som hanteras i "sin verksamhet". Detta ansvar ska gälla på samma sätt som för personuppgiftsansvarig och/eller biträde enligt GDPR.

I avsnittet "Ansvar enligt GDPR" nedan anges kortfattat vilket ansvar som gäller för personuppgiftsansvariga respektive personuppgiftsbiträde enligt GDPR (avsnitt 8.2). Det är detta ansvar som jag som dataskyddsombud (DSO) utgår ifrån när jag bedömer regelefterlevnadsrisker till följd av brister i dataskyddsarbetet i denna rapport.

Som DSO har jag som huvudsaklig uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad. Jag ska lämna information och råd till verksamheten och de anställda om deras skyldigheter enligt GDPR vid behandling av personuppgifter. Uppdraget ska utföras på ett oberoende sätt. Jag ska vidare rapportera status för dataskyddsarbetet direkt till högsta förvaltningsnivå, vilket görs genom denna årsrapport.

I årsrapporten redogör jag som DSO för de granskningar och andra observationer som jag gjort när det gäller verksamhetens status avseende integritet och dataskydd. Årsrapporten är avsedd att ge er som ansvarig för dataskyddsarbetet i verksamheten ett underlag som ni kan använda för uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

# Innehåll

<b>1.</b>	<b>Bakgrund .....</b>	<b>3</b>
<b>2.</b>	<b>Sammanfattning.....</b>	<b>5</b>
2.1	De två viktigaste åtgärderna enligt DSO.....	5
2.2	Översiktlig bedömd status för olika rapporteringsområden .....	6
<b>3.</b>	<b>Presentation av DSO och arbetssätt.....</b>	<b>8</b>
<b>4.</b>	<b>Obligatoriska rapporteringsområden .....</b>	<b>9</b>
4.1	Registerförteckning.....	9
4.2	Styrdokument.....	11
4.3	Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar .....	12
4.4	Konsekvensbedömningar .....	13
4.5	Individens rättigheter.....	15
4.6	Personuppgiftsincidenter .....	16
<b>5.</b>	<b>Gjorda observationer under året.....</b>	<b>17</b>
5.1	Ansvarsskyldigheten .....	18
5.2	Information till den registrerade externt .....	21
5.3	Information till den registrerade internt .....	22
5.4	Stadengemensamma tjänster.....	24
5.5	Information om och kontaktuppgifter till DSO .....	26
<b>6.</b>	<b>Planerade/Föreslagna granskningsområden under det nya verksamhetsåret .....</b>	<b>28</b>
6.1	Sammanfattning.....	28
6.2	Planerade granskningar.....	28
<b>7.</b>	<b>Övrigt att rapportera .....</b>	<b>29</b>
7.1	Sammanfattning.....	29
7.2	Syfte .....	29
7.3	Övriga observationer.....	29
7.4	Råd och rekommendationer .....	29
<b>8.</b>	<b>Ansvar enligt GDPR.....</b>	<b>30</b>
8.1	Ansvar och roller inom Staden.....	30
8.2	Närmare om GDPR:s krav på ansvarig och biträde .....	33
	Bilaga 1 .....	36
	<b>Begäran om uppgifter inför GDPR- årsrapport 2024.....</b>	<b>36</b>

## 2. Sammanfattning

### 2.1 De två viktigaste åtgärderna enligt DSO

#### 2.1.1 Grundläggande översyn av förutsättningarna för ett systematiskt hållbart dataskyddsarbete i löpande förvaltning

Idrottsförvaltningen har en verksamhet som i de flesta fall endast innehåller personuppgifter där det är en låg risk ur ett dataskyddsperspektiv. Det finns undantag exempelvis vid användning av kameraövervakning och personuppgiftsbehandling inom HR-området när det gäller den egna personalen.

Förutsättningarna att kunna axla samtliga krav som ställs på oss enligt GDPR borde vara möjligt att klara inom förvaltningen då verksamheten är begränsad. Antalet anställda gör att det hanteras personuppgifter i stor omfattning internt varför jag föreslår att det genomförs en organisatorisk förstärkning av dataskyddsarbetet.

Det behöver utses en kontaktperson för dataskydd på varje avdelning.

Dataskyddssamordnaren bör ges ansvar att utveckla dataskyddsarbetet inom förvaltningen med hjälp av de utsedda kontaktpersonerna. Dataskyddssamordnaren bör få utbildning i GDPR och kringliggande lagstiftning samt i riktlinjer från EU i den omfattning som verksamheten kräver. Dataskyddssamordnaren bör ha dataskydd som huvudinriktning för att kunna utveckla dataskyddsarbetet i samverkan med DSO.

Vid en organisationsförändring kommer behovet även av DSO:s tjänster att öka. DSO-rollen bör öka från dagens ca 5 % till i vart fall 15 % av heltid för att ge utrymme för att kartlägga alla viktiga personuppgiftsbehandlingar som sker i verksamheten samt för att ge möjlighet till att lämna information och genomföra allmänna utbildningsinsatser om de krav som GDPR ställer upp för olika delar av verksamheterna inte minst för chefer i linjen.

De chefer i verksamheten som ansvarar för behandlingarna med högre risk bör även få utbildning i dataskyddsfrågor.

Ledningen bör informeras om de krav som ställs på förvaltningen när det gäller ett fungerande dataskyddsarbete. Ledningen bör vidare vara aktiv i sin roll som informationsägare inom Staden för att få till stånd en bättre informationsdelning med alla objektägare

för staden-gemensamma IT-tjänster som hanterar information som förvaltningen ansvarar för så att skyddsnivån är tillräcklig och kan bibehållas över tid..

### 2.1.2 Grundlig översyn av intern och extern information om personuppgiftsbehandlingar

GDPRs krav på transparens (art. 12-14) är omfattande och den externa informationen om personuppgiftsbehandlingarna har inte stämts av mot de behandlingar som sker i verksamheten på flera år.

När det gäller transparensen över de behandlingar som sker internt inom Staden och som gäller de egna anställda (och konsulter) är bristerna omfattande. Här krävs det att personuppgiftsbehandlingarna kartläggs och att intern information tas fram. Informationen föreslås publiceras på intranätet på motsvarande sätt som den externa informationen. Det är viktigt att det är lätt att få tillgång till informationen även när det gäller anställda (och konsulter) verksamma inom Staden.

## 2.2 Översiktlig bedömd status för olika rapporteringsområden

Rapporteringsområde		Mindre	Omfattande	Allvarlig
<b>Obligatoriska</b>				
Registerförteckning			X	
Styrdokument		X		
Informationsklassning (Organisatoriska och tekniska åtgärder)			X	
Konsekvensbedömning			X	
Individens rättigheter	X			
Personuppgiftsincidenter	X			
<b>Övriga observationer</b>				
Ansvarsskyldigheten			X	
Information till registrerad extern			X	
Information till registrerad intern			X	
Stadengemensamma tjänster			X	
DSO			X	

(För specificering se respektive avsnitt)

Bedömningsmall för dataskyddsrisiker:

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	

### **3. Presentation av DSO och arbetssätt**

Mitt namn är Christian Sandell och jag är dataskyddsombud inom fem förvaltningar (Arbetsmarknadsförvaltningen, Idrottsförvaltningen, Kulturförvaltningen, Kyrkogårdsförvaltningen och Serviceförvaltningen) sedan mitten av september i år, på halvtid, vilket medför att jag haft begränsad tid för att på djupet lära känna alla delar av dataskyddsarbetet som sker inom förvaltningarna och inom Staden. Jag har expertkunskaper inom GDPR med följdlagstiftning och praxis och har sedan ikraftträdandet i maj 2018 arbetat med dataskyddsfrågor på heltid som dataskyddsombud och som dataskyddsansvarig främst inom privat sektor.

För mig handlar dataskyddsarbete om att visa respekt för de människor vars personuppgifter vi samlar in och hanterar för olika syften.

När vi använder besökandes, kunders och anställdas personuppgifter måste vi ha kunskap om och kontroll över personuppgifterna. Vi ska kunna skydda dem genom ett organiserat arbetssätt, säkra systemlösningar och ansvarstagande samarbetspartners. Dataskyddsarbetet är en kontinuerlig process där vi regelbundet ska ompröva all användning av personuppgifter så att vi inte behandlar mer uppgifter än som är nödvändigt för att nå de ändamål som vi samlade in uppgifterna för. Vi ska även löpande bedöma riskerna för de registrerades friheter och rättigheter inklusive skyddet av personuppgifter. Vi ska informera kunder och anställda om alla våra behandlingar på ett öppet och tydligt sätt. Utgångspunkten för dataskyddsarbetet är en uppdaterad registerförteckning som ger överblick och kontroll och där det framgår vem som är ansvarig för respektive behandling.

Som DSO har jag samlat information om hur vi behandlar personuppgifter inom förvaltningarna och inom Staden. Detta är ett viktigt led i arbete för att jag ska kunna ge råd och stöd om skyldigheterna enligt GDPR till verksamheten.

En av de främsta uppgifterna som DSO har är att övervaka efterlevnaden av GDPR inom verksamheten och hur vi följer våra interna strategidokument. Jag har utgått från Stadens styrande dokument för att förstå hur ansvaret har fördelats och har försökt sammanställa ansvar och roller inom Staden i ett avslutande kapitel (8.1) nedan. Slutsatsen blir att huvudansvaret för dataskyddsarbetet har lagts på respektive nämnd inom Staden.



## 4. Obligatoriska rapporteringsområden

I årsrapporten kommer de sex obligatoriska rapporteringsområden att redovisas även om de enligt mig borde ha justerats över tid då dataskyddsarbetet är en pågående process där bedömningskriterierna måste justeras löpande i takt med att arbetet med dataskyddsfrågorna utvecklas inom en verksamhet och där verksamheten mognar i sin dataskyddsförmåga.

De obligatoriska rapporteringsområdena är registerförteckning, styrdokument, informationsklassning (som en del av tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar), konsekvensbedömningar, individens rättigheter och personuppgiftsincidenter. Dessa rapporteringsområden har varit samma sedan de infördes.

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

Som ett led i uppföljningen har verksamheten fått svara på ett antal frågor som DSO skickade ut. Frågor och svar framgår av bilaga 1. De svar som har lämnats på dessa frågor av verksamheten har beaktats i den nedanstående bedömningen av respektive område.

### 4.1 Registerförteckning

#### 4.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	93
Har nödvändiga uppdateringar gjorts?	Endast en registrering är uppdaterad under 2024
Bedöms registerförteckningen vara fullständig?	Nej det verkar sakna processer inom HR-området och kamerabevakning m.m.

Har verksamheten lämpliga rutiner för registerföring?

Det finns en rutin för att hantera registreringar där chefer i verksamheter är ansvariga

#### 4.1.2 Syfte

Förteckning över behandlingar, även kallad behandlingsregistret eller registerförteckning, är ett direkt lagkrav 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 förvaltningens registerförteckning.

#### 4.1.3 Resultatet av genomgången

Det finns ett behandlingsregister som omfattar processer som är hänförliga till den verksamhet som förvaltningen driver. Däremot saknar det uppgifter om behandlingar/processer inom HR-området som är ett av de områden där det finns högre risk än inom övriga delar av verksamheten. Såvitt kan bedömas saknas även processer där det finns bildupptagning och bevakningskameror.

#### 4.1.4 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

#### 4.1.5 DSO ger råd och rekommendationer till PUA

Då de delar av behandlingsregistret som rör de behandlingar där riskerna är störst, är eftersatt är det angeläget att fokus riktas mot den delen av förteckningen. Registerförteckningen bör vidare revideras med årlig intervall.

## 4.2 Styrdokument

### 4.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Ja delvis
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Ja men frågan är om de visar verkligheten
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Ja
Är dokumenten uppdaterade?	Det finns behov av att se över vissa dokument
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja såvitt kan bedömas

### 4.2.2 Syfte

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 förvaltningens styrdokument inom dataskydd.

### 4.2.3 Resultatet av genomgången

Det finns ett dokument som är från 2022 som avser "Informationssäkerhet och dataskydd på idrottsförvaltningen" Där finns det en gruppering som kallas Informationssäkerhets- och dataskyddsgrupp

Deltagare:

- \* IT-chef, ordförande och sammankallande
- \* Informationssäkerhetssamordnare
- \* Systemadministratör säkerhet
- \* Registrator
- \* Dataskyddssamordnare
- \* Kommunikatör
- \* Säkerhetssamordnare

Denna gruppering borde kunna driva dataskyddsarbetet, men jag ifrågasätter om den är verksam. I Ledningens genomgång år 2023 finns det ett starkt fokus på dataskydd.

Delegationsordningen bör justeras då det där står att det är DSO som ska ansvara för registerförteckningen. Där står även att personuppgiftsincidenter som ska anmälas till Integritetsskyddsmyndigheten ska anmälas till nämnden. (Jag vet inte vad den delegationen vill reglera.)

(Jag kan inte hitta dokumentet ”Lokal anvisning för informationssäkerhetsarbete” som skulle tas fram under 2023 eller i början av 2024 varför jag har svårt att till fullo bedöma det styrdokumentet.)

#### 4.2.4 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

#### 4.2.5 DSO ger råd och rekommendationer till PUA

Det finns styrande dokument som är anpassade för idrottsförvaltningens verksamhet även om de behöver ses över. En annan fråga blir om styrdokumenterna stämmer överens med hur organisationen av informationssäkerhets- och dataskyddsarbetet är organiserat. Lokal anvisning för informationssäkerhet bör finnas på intranätet under Informationssäkerhet.

### 4.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

#### 4.3.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	Totalt är ca 20 processer klassade och 3 har genomförts under 2024. Processer inom HR området bör informationsklassas.
Är klassade personuppgiftsbehandlingar aktuella?	Det finns ingen rutin att riskbedöma äldre behandlingar

#### 4.3.2 Syfte

För att kunna skydda information som även omfattar personuppgifter med rätt slags skydd så ska verksamheten informationsklassa sin information. Informationsklassning av information och av system är viktiga byggstenar för att kunna bedöma om personuppgiftsbehandlingen är skyddad på rätt sätt. Syftet med detta avsnitt är att bedöma rutinerna kring informationsklassning med hänsyn till de personuppgiftsbehandlingar som hanteras inom förvaltningen.

#### 4.3.3 Resultatet av genomgången

Det känns som om infoklassningar och riskbedömningar inte har genomförts i den grad som styrdokumenterna visar. Se särskilt ledningens genomgång. Även hela HR-området behöver ses över.

#### 4.3.4 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

#### 4.3.5 DSO ger råd och rekommendationer till PUA

Informationssäkerhetsarbetet behöver ske löpande. Det finns behov av att göra en översyn av HR-området ur ett riskperspektiv.

### 4.4 Konsekvensbedömningar

#### 4.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	En har hittats och påbörjats gällande föreningsstöd- och bokningsstöd.
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Då HR-området ej finns med i registerförteckningen så kan det finnas behov av en grundlig genomgång
Är de genomförda bedömningarna aktuella?	Saknas rutin för att förnya tröskel och konsekvensbedömningarna

#### 4.4.2 Syfte

En konsekvensbedömning är nödvändig när det bedöms att en behandling kan innebära en hög risk för registrerades friheter och rättigheter. 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 för en registrerad 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 skyddsåtgärder för att sänka risken. Dessa skyddsåtgärder kan vara tekniska eller organisatoriska

För att få en uppfattning om en personuppgiftsbehandling innebär en hög risk ska normalt alla personuppgiftsbehandlingar genomgå en så kallad "träskelanalys". Vid träskelanalysen bedöms om kriterier för hög risk enligt GDPR (art. 35) och enligt IMY:s riktlinjer är aktuella. Om så är fallet så är det nödvändigt att genomföra en konsekvensbedömning.

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

#### 4.4.3 Resultatet av genomgången

Det finns sannolikt fler behandlingar som kommer kräva en konsekvensbedömning efter genomförd Träskelanalys.

#### 4.4.4 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

#### 4.4.5 DSO ger råd och rekommendationer till PUA

Hela HR-området behöver informationsklassas och träskelanalyser behöver genomföras så att eventuella konsekvensbedömningar kan planeras och genomföras.

## 4.5 Individens rättigheter

### 4.5.1 Sammanfattning

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

### 4.5.2 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. När en begäran kommit in från en registrerad ska det finnas rutiner så att begäran kan hanteras av verksamheten inom 30 dagar.

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

### 4.5.3 Resultat av genomgången

Det finns en rutin och utsedda handläggare som får bedömas som tillfredsställande. Någon kontroll av en begäran har dock inte genomförts under min tid som DSO.

### 4.5.4 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

### 4.5.5 DSO ger råd och rekommendationer till PUA

Det finns rutiner på plats och utpekade handläggare vilket är tillfredsställande med hänsyn till inriktningen av verksamheten.

## 4.6 Personuppgiftsincidenter

### 4.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Oklart
Hur många personuppgiftsincidenter har dokumenterats?	Saknar sammanställning
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Ingen
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	-

### 4.6.2 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 inom förvaltningen.

En personuppgiftsincident ska normalt anmälas till Integritetsskyddsmyndigheten, IMY, inom 72 timmar. Anmälan till IMY behöver inte ske om den personuppgiftsansvarige kan visa att det är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter.

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

### 4.6.3 Resultat av genomgången

Det finns rutiner för att rapportera incidenter. Med hänsyn till omfattningen av verksamheten borde det vara några incidenter som borde anmälts till IMY med hänsyn till den låga tröskeln för anmälan när det gäller risken för en fysisk persons friheter och rättigheter.



#### 4.6.4 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
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	Inga brister av nämnvärd betydelse identifierade

#### 4.6.5 DSO ger råd och rekommendationer till PUA

Då det kan finnas risk att det sker en underrapportering av incidenter är det viktigt att den grundläggande utbildningen i dataskydd genomförs då den bland annat tar upp incidentfrågorna på ett bra sätt.

## 5. Gjorda observationer under året

1. Ansvarsskyldigheten
2. Information till den registrerade externt
3. Information till den registrerade internt
4. Stadengemensamma tjänster
5. Information om och kontaktuppgifter till DSO

Som nytt dataskyddsombud har jag haft anledning att ta reda på hur dataskyddsarbetet ser ut inom Staden och i den egna förvaltningen. Jag har gått in på Stadens externa sidor och observerat hur information har presenterats för en besökare. Jag har även gått in på de interna sidorna och gjort motsvarande observationer av hur dataskyddsfrågor hanterats och vilken information som funnits där. Jag har även gjort observationer på lokala samarbetsytter och i samband med olika möten och samtal med personer inom Staden och i förvaltningen.

Vid dessa genomgångar har jag stött på olika frågeställningar där jag har känt att det finns brister och oklarheter som behöver hanteras på olika sätt men att det av olika skäl inte funnits tid för att ta hand om varje enskild brist direkt. Även positiva observationer har gjorts. Då jag har en ambition att vilja se ett gott dataskyddsarbete inom förvaltningen (men även inom de andra förvaltningar där jag är DSO) har jag valt att i denna årsrapport flagga upp att det finns flera områden (utöver de obligatoriska) där det finns en tydlig förbättringspotential så att nämnden, ledningen

och dataskyddsorganisationen inom förvaltningen kan ta frågorna vidare.

## 5.1 Ansvarsskyldigheten

	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

### 5.1.1 Grundläggande krav enligt GDPR

Enligt GDPR (art 5:2) har den personuppgiftsansvarige ett ansvar för att alla grundläggande dataskyddsprinciper efterlevs gällande all personuppgiftsbehandling i en verksamhet. Den personuppgiftsansvarige ska vidare (se art 24:1) med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa att behandlingen utförs i enlighet med GDPR. Dessa åtgärder ska ses över och uppdateras vid behov. Den personuppgiftsansvarige ska vidare kunna visa att all behandlingen utförs i enlighet med GDPR. Det innebär att alla frågor och andra överväganden som rör arbetet med dataskydd behöver dokumenteras för framtiden.

### 5.1.2 Observation

Som personuppgiftsansvarig men även som biträde har varje nämnd det operativa ansvaret för att verksamheten är organiserad och har tillräckliga resurser för att kunna leva upp till GDPR:s krav vid all hantering av personuppgifter inom sin verksamhet.

Staden har valt att lägga in dataskyddarbetet som en del inom arbetet med informationssäkerhet. Även om det finns tydliga beröringspunkter mellan dessa regelverk så finns det delar av dataskyddsarbetet som ställer andra krav och som i vissa delar (såsom reglerna i GDPR är utformade) kan hamna i strid med vad som anses som bra informationssäkerhet. Dataskyddsarbete avser att skydda de registrerades friheter och rättigheter till skillnad mot informationssäkerhet som avser att skydda verksamhetens informationstillgångar.

Dataskyddsarbetet inom Staden har efter att införandeprojektet avslutades 2019 formats lokalt inom respektive förvaltning vilket har medfört att delar av dataskyddsarbetet fungerar men att andra delar har försummats eller inte har beaktats.

Enligt Staden har Informationssäkerhetssamordnaren (ISAM) och DSO ansetts vara de personer/funktioner som haft ansvaret att driva dataskyddsarbetet framåt från start. Denna uppfattning har hämmat utvecklingen då DSO inte både kan ha det operativa ansvaret och samtidigt agera på oberoende basis och granska samma dataskyddsarbete. Trots att Stadsrevision i sin granskning redan 2019 (av implementeringen av dataskyddsarbetet) poängterade att ”dataskyddsombudet ska ha en reviderande och rådgivande roll och inte delta i det operativa arbetet med behandling av personuppgifter som t.ex. inventering och upprättande av registerförteckning.”(se sid 5 i Stadsrevisions rapport nr 5, 2019) så gick utvecklingen åt ett annat håll.

När det gäller förvaltningen så finns det fortfarande delar i rutiner och anvisningar som pekar ut DSO som drivande i olika delar av dataskyddsarbetet. Delegationsordningen anger att DSO ska ”ansvara” för registerförteckningen vilket står i strid med lagstiftningen.

I dokumentet från 2022 som avser ”Informationssäkerhet och dataskydd på idrottsförvaltningen” finns det en gruppering som kallas Informationssäkerhets- och dataskyddsgrupp

Deltagare:

- \* IT-chef, ordförande och sammankallande
- \* Informationssäkerhetssamordnare
- \* Systemadministratör säkerhet
- \* Registrator
- \* Dataskyddssamordnare
- \* Kommunikatör
- \* Säkerhetssamordnare

Om denna gruppering skulle vara aktiv så finns det möjligheter att hantera de krav som GDPR ställer för verksamheten. I Ledningens genomgång år 2023 finns det vidare ett starkt fokus på dataskydd. I de svar som lämnats kring de obligatoriska områdena inför denna rapport men även vid kontakter med förvaltningen har det framgått att delar av de aktiviteter som skulle genomföras 2024 inte kommit att genomföras.

För Idrottsförvaltningens del är dataskyddsarbetet koncentrerat till två personer, dataskyddssamordnaren och ISAM, som båda har andra huvudsakliga uppgifter. Vidare är ansvaret utspritt och varje

chef inom verksamheten har ansvar för att sin information i verksamheten hanteras lagligt. Även andra personer inom förvaltningens verksamheter har uppgifter som rör dataskyddsarbetet men det saknas någon som kan vara en kunskapskälla och pådrivare med huvudsaklig inriktning mot dataskydd.

Även min roll som DSO har begränsningar då en halvtid ska räcka för att stödja verksamheten inom fem förvaltningar vilket är klart begränsande.

### **5.1.3 Råd och rekommendation**

Idrottsförvaltningen har en verksamhet som i de flesta fall endast innehåller personuppgifter där det är en låg risk ur ett dataskyddsperspektiv. Det finns dock undantag exempelvis vid användning av kameraövervakning och personuppgiftsbehandling inom HR-området när det gäller den egna personalen.

I min bedömning utgår jag från de krav som GDPR ställer upp på en personuppgiftsansvarig (se avsnitt 8.2) varför jag drar slutsatsen att verksamheten inte är organiserad, ur ett dataskyddsperspektiv, så att den kan klara av att leva upp till alla krav som ställs. Ansvarsskyldigheten är omfattande och det är nödvändigt att dataskyddsarbetet är organiserat och bemannat så att dataskyddsfrågorna kan hanteras löpande i verksamheten och även hållbart över tid.

Då dataskyddsarbetet vid min bedömning verkar ha tappat fokus är det nödvändig att rekommendera förändringar.

Det är viktigt att påpeka att de personer som jag haft kontakt med och samverkat med har alla visat på god vilja att förstå och arbeta för att förbättra dataskyddsarbetet inom förvaltningen.

Förutsättningarna att kunna axla samtliga krav som ställs på oss enligt GDPR borde vara möjligt att klara inom förvaltningen då verksamheten är begränsad. Antalet anställda gör att det hanteras personuppgifter i stor omfattning internt varför jag föreslår att det genomförs en organisatorisk förstärkning av dataskyddsarbetet.

Det behöver utses en kontaktperson för dataskydd på varje avdelning.

Dataskyddssamordnaren bör ges ansvar att utveckla dataskyddsarbetet inom förvaltningen med hjälp av de utsedda kontaktpersonerna. Dataskyddssamordnaren bör få utbildning i GDPR och kringliggande lagstiftning samt i riktlinjer från EU i den omfattning som verksamheten kräver.

Dataskyddssamordnaren bör ha dataskydd som huvudinriktning för att kunna utveckla dataskyddsarbetet i samverkan med DSO.

Vid en organisationsförändring kommer behovet även av DSOs tjänster att öka. DSO-rollen bör öka från dagens ca 5 % till i vart fall 15 % av heltid för att ge utrymme för att kartlägga alla viktiga personuppgiftsbehandlingar som sker i verksamheten samt för att ge möjlighet till att lämna information och genomföra allmänna utbildningsinsatser om de krav som GDPR ställer upp för olika delar av verksamheterna inte minst för chefer i linjen.

De chefer i verksamheten som ansvarar för behandlingarna med högre risk bör även få utbildning i dataskyddsfrågor.

Ledningen bör informeras om de krav som ställs på förvaltningen när det gäller ett fungerande dataskyddsarbete. Ledningen bör vidare vara aktiv i sin roll som informationsägare inom Staden för att få till stånd en bättre informationsdelning med alla objektägare för staden-gemensamma IT-tjänster som hanterar information som förvaltningen ansvarar för så att skyddsnivån är tillräcklig och kan bibehållas över tid.

## 5.2 Information till den registrerade externt

	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

### Krav enligt GDPR

Informationskraven enligt GDPR kring personuppgiftsbehandlingar är omfattande (art 12-14) och är en viktig fråga kring transparensen i dataskyddsarbetet.

Informationskraven gäller alla typer av behandlingar hos en personuppgiftsansvarig. Informationen ska vara tydlig och begriplig så att du vet vilka uppgifter som används för vilket ändamål och grund för respektive personuppgiftsbehandling. Det ska även framgå vem informationen delas med och inte minst hur länge personuppgifterna sparas. Även användning av personuppgiftsbiträden ska framgå och om det förekommer att

personuppgifter överförs till tredje länder, det vill säga utanför EU/EES.

Att lämna en tydlig utformad information till den registrerade är en förutsättning för att kunna behandla personuppgifterna överhuvudtaget (med få undantag).

Informationen ska vara klar och tydlig och ska tillhandahållas den registrerade i god tid före det att behandlingen sker exempelvis vid insamlandet av uppgifterna eller senast inom 30 dagar från insamlandet eller om behandlingen sker dessförinnan senast vid behandlingen.

Informationen ska även utförligt ta upp hur de registrerade kan ta tillvara sina rättigheter och möjlighet att klaga. Där ska även dataskyddsombudets kontaktuppgifter framgå.

Det finns en riktlinje som tagits fram på EU-nivå med utförliga anvisningar om hur informationen ska presenteras (Riktlinjer om öppenhet, WP260rev0.1) samt åtskilliga beslut och rättsfall inom EU som visar nivån på öppenheten.

### 5.2.1 Observation

Det finns ingen särskilt framtagen information om behandling av personuppgifter som publicerats på Stadens hemsida när det gäller Idrottsförvaltningen.

### 5.2.2 Råd och rekommendation

Med hänsyn till omfattningen på verksamheten och även att det finns flera typer av bildupptagningar i verksamheterna runt om i staden så är det nödvändigt att det finns en tydlig information över de behandlingar som faktiskt sker. Den ska vara detaljera och lättillgänglig då målgruppen är barn och unga i stor utsträckning.

## 5.3 Information till den registrerade internt

	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

### 5.3.1 Krav enligt GDPR

Informationskraven enligt GDPR kring personuppgiftsbehandlingar är omfattande (art 12-14) och är en viktig fråga kring transparensen i dataskyddsarbetet.

Informationskraven gäller alla typer av behandlingar hos en personuppgiftsansvarig. Informationen ska vara tydlig och begriplig så att du vet vilka uppgifter som används för vilket ändamål och grund för respektive personuppgiftsbehandling. Det ska även framgå vem informationen delas med och inte minst hur länge personuppgifterna sparas. Även användning av personuppgiftsbiträden ska framgå och om det förekommer att personuppgifter överförs till tredje länder, det vill säga utanför EU/EES.

Att lämna en tydlig utformad information till den registrerade är en förutsättning för att kunna behandla personuppgifterna överhuvudtaget (med få undantag).

Informationen ska vara klar och tydlig och ska tillhandahållas den registrerade i god tid före det att behandlingen sker exempelvis vid insamlandet av uppgifterna eller senast inom 30 dagar från insamlandet eller om behandlingen sker dessförinnan senast vid behandlingen.

Informationen ska även utförligt ta upp hur de registrerade kan ta tillvara sina rättigheter och möjlighet att klaga. Där ska även dataskyddsombudets kontaktuppgifter framgå.

Det finns en riktlinje som tagits fram på EU-nivå med utförliga anvisningar om hur informationen ska presenteras (Riktlinjer om öppenhet, WP260rev0.1) samt åtskilliga beslut och rättsfall inom EU som visar nivån på öppenheten.

### 5.3.2 Observation

Informationskraven gäller även för behandlingar som sker internt hos en personuppgiftsansvarig.

Inom HR-området förekommer en stor mängd behandlingar som rör dels underställda registrerade i form av anställda dels känsliga eller i vart fall integritetskänsliga uppgifter även det i stor omfattning. När det gäller anställda så kan det även förekomma att det sker bildupptagningar genom övervakningskameror och ljudinspelningar vid samtal med kunder eller mellan medarbetare i olika interna tjänster. Generellt är informationen om behandlingar som sker inom Staden och även inom nämndens verksamhet ytterst bristfällig.

### 5.3.3 Råd och rekommendation

Det är viktigt att dessa behandlingar informeras tydligt om på intranätet på samma sätt som är normalt gällande den externa hemsidan. Även förekomst av cookies och annan spårning internt är viktigt att informera om.

Informationen ska även utförligt ta upp hur de registrerade kan ta tillvara sina rättigheter och möjlighet att klaga. Där ska även dataskyddsombudets kontaktuppgifter framgå.

## 5.4 Stadengemensamma tjänster

	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

### 5.4.1 Krav enligt GDPR

GDPR utgår ifrån att såväl personuppgiftsansvarig som biträde har organisatoriska och tekniska åtgärder på plats för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken för fysiska personers rättigheter och friheter vid all behandling (art. 32)

### 5.4.2 Observation

Inom staden har man delat upp ansvaret ur ett informationssäkerhetsperspektiv när det gäller olika typer av IT-tjänster även om de används av samtliga nämnder inom staden. Ur ett dataskyddsperspektiv ska varje förvaltning i egenskap av informationsägare, som vill bruka en IT-tjänst, göra nya riskbedömningar och konsekvensbedömningar utifrån den information som man avser att hantera i IT-Tjänsten. Detta förhållande är särskilt uttalat i centralt styrande dokument. Då tjänsterna oftast är upphandlade borde det finnas genomförd informationsklassning och framtagna upphandlingskrav och även ett gällande tjänsteavtal med SLA och personuppgiftsbiträdesavtal med instruktioner och krav på säkerhetsskydd. Även en processbeskrivning borde finnas tillgänglig.

I flera fall har det framkommit att det är svårt att som informationsägare få tillgång till dessa underlag som legat till grund för den ursprungliga anskaffningen av IT-tjänsten. Denna information borde finnas samlad hos objektägaren eller i



objektstyrgruppen. Det borde även gälla för IT-tjänster som ligger externt.

Då det är objektägaren för IT-tjänsten som ansvarar för informationssäkerhetsarbetet som avser drift underhåll och utveckling av IT-tjänsten (Tillämpningsanvisning till stadens riktlinje för informationssäkerhet, 1.4.2) så bör det, trots att det inte är uttalat, ändå vara objektägaren som ansvarar för dataskyddsfrågorna som har samband med IT-tjänsten.

Problemen med delat ansvar i en fråga är att det ofta uppstår problem med att få information som är nödvändig för att med eget ansvar veta om information kan hanteras säkert i en IT-tjänst där det saknas underlag för att veta exempelvis hur tjänsten är utformat, var information hämtas ifrån och hur den processas, hur slutresultatet delas.

Även underleverantörer bör det finnas information om då det kan ha betydelse när det gäller tredjelandsöverföringar och annat.

Det är en återkommande fråga bland annat i Dataskyddssamverkansgruppen (GUG) att det är svårt att få fram nödvändiga underlag när det är dags för informationsägaren att genomföra sin riskanalys och konsekvensbedömning för att kunna bedöma om det går att använda IT-tjänsten för den personinformation man svarar för.

Under 2024 har inställningen inom Staden ändrats i detta avseende och så kallade normerande klassningar har påbörjats avseende gemensamma IT-tjänster. Avsikten är att även informationsägarnas krav ska beaktas i samband med riskbedömning och klassning. Även om det inte är uttalat i styrdokumentet bör konsekvensbedömning sannolikt ingå i förfarandet.

En stor del av stadens behandlingar särskilt när det gäller alla behandlingar inom HR-området är av detta slag och här finns det stora osäkerhet hur status är när det gäller såväl informationssäkerhet som skydd för personuppgifter.

### **5.4.3 Råd och rekommendation**

Det är väsentligt för förvaltningen att ha ordning på alla personuppgiftsbehandlingar ur ett dataskyddsperspektiv varför det är nödvändigt att ha en organisation som kan få fram ovan angivna underlag för att kunna riskbedöma de behandlingar som sker i centrala IT-system.

Informationsägare bör, via förvaltningschef eller ansvarig för dataskydd, följa upp frågan och ställa krav på att samtliga

underlag av denna typ av IT-tjänst är samlad och tillgängliga för berörda informationsägare om ansvaret ska ligga lokalt hos förvaltningen.

## 5.5 Information om och kontaktuppgifter till DSO

	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

Varje nämnd i Stockholms stad har utnämnt ett DSO som anmäls till Integritetsskyddsmyndigheten ("IMY"). Genom att utse och anmäla in ett DSO till IMY gäller GDPR:s regler i förhållandet mellan nämnden och DSO (GDPR art. 37-39 samt Riktlinje om dataskyddsbud (WP 243/2016)).

### 5.5.1 Krav enligt GDPR

Av GDPR (art. 38.4-5) framgår det att den registrerade får kontakta DSO med avseende på alla frågor som rör behandlingen av dennes personuppgifter och utövandet av dennes rättigheter enligt GDPR. DSO ska när det gäller genomförande av sina uppgifter vara bundet av sekretess bland annat i enlighet med svensk rätt. I dataskyddslagen (SFS 2018:218, 8 §) anges att DSO inte obehörigen får röja det som han eller hon vid fullgörandet av sin uppgift har fått kännedom om. Denna tystnadsplikt förutsätter att en registrerad ska kunna komma i kontakt med DSO och lämna information utan att DSO får föra informationen vidare annat än om den registrerade givit sitt samtycke. Då det kan röra sig om en registrerad som är anställd är tystnadsplikten viktig att upprätthålla för att skydda den anställda.

GDPR ställer även krav på att DSO:s kontaktuppgifter ska offentliggöras.

### 5.5.2 Observation

Det finns en sida på Stadens hemsida som heter Dataskyddsbud där det lämnas information om vem som är DSO i enskilda förvaltningar och kontaktuppgifter till DSO.

Denna sida innehåller ofta fel uppgifter när det gäller vem som är DSO och det är vidare vanligt att den e-postadress som anges inte är en kontaktväg till DSO utan vanligtvis är den funktionsbrevlåda som kommit att bli den allmänna kontaktvägen till dataskyddsorganisationen och inte exklusivt till DSO.

När det gäller Idrottsförvaltningen är det fel uppgift på vem som är DSO. Den e-postadressen, som borde gå direkt till DSO, är den normala e-postadressen som går till förvaltningen: ”idrott@stockholm.se”.

### **5.5.3 Råd och rekommendationer**

Det ska vara möjligt att kontakta DSO utan att någon annan får veta att den registrerade kontaktat DSO. Det bör lämpligen finnas två kontaktuppgifter på den aktuella sidan dels en e-post där registrerad kan begära att få registerutdrag och liknande begäran dels en e-post där en registrerad kan komma i direktkontakt med DSO.

## **6. Planerade/Föreslagna granskningsområden under det nya verksamhetsåret**

### **6.1 Sammanfattning**

Relevanta granskningsområden inom verksamheten:

- Uppföljning av organisationen för det strukturella dataskyddsarbetet
- Uppföljning av informationen om personuppgifterna externt och internt särskilt kamerabevakning.
- Genomgång av utbildningsmaterial som finns för att rekommendera utbildningsåtgärder för att växla upp dataskyddsarbetet.
- Utvärdera registerutdragsprocessen.

### **6.2 Planerade granskningar**

Då det är osäkert om jag kommer att fortsätta som dataskyddsombud inom förvaltningen under nästa år så är det svårt att planera för fortsatta granskningar i detalj.

## 7. Övrigt att rapportera

### 7.1 Sammanfattning

Det är viktigt att den obligatoriska dataskyddsutbildningen som finns genomgås årligen av alla medarbetare och konsulter.

### 7.2 Syfte

För att skapa en bra dataskyddskultur inom en förvaltning är utbildning och information om dataskyddsregelverket viktigt att presentera på ett verksamhetsnära sätt.

### 7.3 Övriga observationer

Den inom Staden framtagna utbildningen ”Dataskydd i kommunal verksamhet, Grundkurs 2022) är väl genomförd i de delar av dataskyddsarbetet som den omfattar med ett undantag som rör DSO:s ansvar. Det är den operativa dataskyddsorganisationen och inte DSO som ska säkerställa att verksamheten följer GDPR.

Utbildningen innehåller i huvudsak:

- Grunder och definitioner
- Grundläggande dataskyddsprinciper
- Rättslig grund
- Registrerades rättigheter
- Allmän handling – GDPR
- Fritext och e-post
- Personuppgiftsincidenter

Utbildningen ska genomföras årligen. I början av december hade ca 18 % av medarbetarna (106/577) på förvaltningen genomfört utbildningen.

### 7.4 Råd och rekommendationer

Det är viktigt att den obligatoriska dataskyddsutbildningen genomgås årligen av alla medarbetare och konsulter då den är bra i de delar av dataskyddsarbetet som den tar upp. Ytterligare utbildningsinsatser behöver övervägas för de funktioner som har ansvar för andra delar av dataskyddsarbetet. Det finns flera framtagna utbildningar inom Staden som kan vara lämpliga att genomgå för utvalda grupper inom förvaltningen.

## 8. Ansvar enligt GDPR

### 8.1 Ansvar och roller inom Staden

Avsikten med detta avsnitt är att försöka få bättre klarhet över de regelverk som styr ansvar och roller kring informationssäkerhet och dataskydd inom Staden som helhet. Det finns vissa styrande dokument som anger huvudriktningen för ansvar och roller som gäller för bland annat alla nämnder. Denna kartläggning är väsentlig för att kunna förstå även det lokala dataskyddsarbetet och veta vem som har ansvar för vad.

#### 8.1.1 Överordnade beslut om informationssäkerhet

Kommunfullmäktige beslutade genom ”Reglemente med allmänna bestämmelser för Stockholm stads nämnder”, 2023:09, 5§, följande:

”Nämnden är personuppgiftsansvarig för de personuppgifter som nämnden behandlar i sin verksamhet. Nämnden kan också vara personuppgiftsbiträde åt en annan nämnd eller gemensamt personuppgiftsansvarig tillsammans med en annan nämnd, varvid de inbördes ansvarsförhållandena ska regleras. Vid ett biträdesförhållande ska den personuppgiftsansvariga nämnden ge instruktioner om behandlingen till den personuppgiftsbiträdande nämnden. Om gemensamt personuppgiftsansvar förekommer ska fördelningen av ansvar regleras mellan nämnderna, bl.a. avseende den registrerades rättigheter och tillhandahållande av information till den registrerade.”

I Riktlinje för informationssäkerhet i Stockholms stad (2022-02-21) som gäller i samtliga nämnder och styrelser står bland annat följande:

Stadens kvalitetsarbete ... ställer krav på att staden utför ett grundläggande och systematiskt informationssäkerhetsarbete i alla sina verksamheter. Denna riktlinje anger kommunfullmäktiges direktiv för detta arbete. Arbetet ska i sin tur bidra till att staden upprätthåller trygghet och förtroende hos medborgare, näringsliv och besökare, men också att lagar, förordningar och riktlinjer efterlevs. Dagens informationssamhälle har lett till att grundläggande samhällsfunktioner är beroende av information i digitala tjänster. Detta beroende innebär i sin tur risker. Därför har kraven på skydd för information skärpts avsevärt genom lagstiftning, exempelvis dataskyddförordningen och NIS-direktivet samt regeringens strategi på nationell nivå. Både stadens ambitioner och svensk lagstiftning förutsätter en ändamålsenlig informationssäkerhet i stadens nämnder och styrelser...

... Dataskydd innebär skydd av personuppgifter enligt kraven i dataskyddsförordningen. Dataskydd är en del av informationssäkerhetsarbetet i staden...

### **8.1.2 Nämnders övergripande ansvar**

I tillämpningsanvisning till stadens riktlinjer för informationssäkerhet (2024-11-13) är nämnder informationsägare och personuppgiftsansvariga för sin verksamhets personuppgiftsbehandling (1.4.2).

Nämnderna ansvarar för att det finns ett ändamålsenligt och effektivt informationssäkerhetsarbete inom den egna verksamheten samt att stadsövergripande riktlinjer och lagkrav efterlevs.

Nämnderna är dessutom i egenskap av personuppgiftsansvarig enligt dataskyddslagstiftningen skyldig att instruera medarbetare m.fl. om hur personuppgifter får behandlas, genom rutiner och instruktioner.

Informationsägare ska fatta beslut om informationens skyddsvärde samt ställa krav på skyddsåtgärder och är ansvarig för att adressera skyddsåtgärder till rätt part. Informationsägaren ska omvärdera skyddsvärdet vid ändrade förhållanden på årlig basis.

En personuppgiftsansvarig är den som bestämmer ändamål och medel för en personuppgiftsbehandling. Inom staden ska det bestämmas vilken nämnd som är ansvarig och vilken som är biträden innan en behandling sker. Om en nämnd utför behandlingen åt en annan nämnd uppstår ett internt personuppgiftsbiträdesförhållande som dock inte kan regleras genom avtal då Staden är en juridisk person. Rollerna, ansvarig, gemensamt ansvarig och biträde behöver bestämmas och regleras så att alla parter vet vem som ska göra vad. Det är även viktigt att tydligt dokumentera dessa förhållanden på en gemensam yta. Vid interna arrangemang där flera nämnder är inblandade så är det viktigt att även informera de registrerade om arrangemanget och hur man kan ta tillvara sina friheter och rättigheter.

### **8.1.3 Förvaltningschefens ansvar**

Förvaltningschef är nämndens operativa informationsägarrepresentant i verksamheten och ansvarar bland annat för att organisera verksamheten så att informationsägaransvaret och personuppgiftsansvaret kan omhändertas i linjen (1.4.2).

Förvaltningschef ska utse en informationssäkerhetssamordnare (nedan ISAM) som leder och samordnar det operativa arbetet med informationssäkerhet inom nämnden.

En Lokal anvisning för informationssäkerhet (1.4.2) ska fastställas av förvaltningschef med beskrivning av hur stadens övergripande ledningssystem för informationssäkerhet omsätts i den egna verksamheten. Den lokala anvisningen ska ses över årligen. Anvisningen ska beskriva ansvarsfördelning och roller inom egen informationssäkerhetsorganisation samt om specifik lagstiftning ska beaktas i verksamheten.

Förvaltningschef beslutar om nödvändiga resurser, mandat och befogenheter för de funktioner som arbetar med informationssäkerhet

#### **8.1.4 Uppföljning av informationssäkerhetsarbetet**

Den årliga rapporten Ledningens genomgång ska sammanställas av ISAM och lämnas till förvaltningschefen och omfatta en genomlysning av informationssäkerhetsarbete och ge underlag för förbättringar inför kommande verksamhetsår. Rapporteringen ska även innefatta dataskydd utifrån vad som framkommer i DSOs GDPR-årsrapport. Förvaltningschefen beslutar aktiviteter inom de två områdena för att uppnå tillräcklig kontroll.

#### **8.1.5 Objektägare och objektstyrgrupp**

Objektägare ansvarar för informationssäkerhetsarbetet i en IT-tjänster utöver ansvar för drift underhåll och utveckling av IT-tjänsten (Tillämpningsanvisning till stadens riktlinje för informationssäkerhet, 1.4.2). Vem som ansvarar för dataskyddsfrågorna som rör IT-tjänster är inte lika tydligt uttalat. Det får antas att det ändå är objektägaren som ansvarar för dataskyddsfrågorna.

Det finns en objektsägare för alla IT-tjänster som hanterar personuppgifter inom Stadens verksamheter. Det gäller även om IT-tjänsten levereras av en extern system- eller tjänsteleverantör. Objektägaren rapporterar till en Objektstyrgrupp som ansvarar för att leda informationssäkerhetsarbetet. Även här är det oklart vem av dessa som ansvarar för allt dataskyddsarbete.

#### **8.1.6 Chefer inom verksamheten**

Ansvar för att skydda information i staden är decentraliserat och innebär att chefer som närmast ansvarar för en verksamhet har del i detta ansvar.

Chefen ansvarar för att den egna verksamhetens informationshantering följer riktlinjer för informationssäkerhet. Därför ska varje chef tillse att det kartläggs vilken typ av information som just deras verksamhet hanterar samt att den mest



betydelsefulla informationen, inte minst känsliga och integritetskänsliga personuppgiftsbehandlingar, är klassade.

Chefen ska tillse att de skyddsåtgärder som följer av klassningen på ett pragmatiskt sätt arbetas in i verksamhetens ordinarie linjearbete. Det ska vara tydligt vem i chefens linjeverksamhet som ansvarar för vilken åtgärd. Med skyddsåtgärder avses exempelvis att en uppföljning av behörigheter sker regelbundet, att en riktlinje eller anvisning tas fram, att personalen är informerad om sitt ansvar för informationssäkerhet med mera

## **8.2 Närmare om GDPR:s krav på ansvarig och biträde**

Det avsnitt som återges nedan har flyttats ut ur Stadens obligatoriska styrdokument "Tillämpningsanvisningar till stadens riktlinje för informationssäkerhet" vid den senaste revideringen som beslutades av stadsdirektören 2024-11-13. Ändringen beskrivs enligt följande: "Minskad omfattning genom att vägledande (ej styrande) textstycken har flyttats ut." I Nyhetsbrev till ISAM uppger Funktionen för stadsövergripande informationssäkerhet att "uppdateringarna förändrar inte innehållet i sak, utan syftar till att förstärka och förtydliga de anvisningar som redan är beslutade".

Då avsnittet är det enda som visar på ansvarsskyldigheten enligt GDPR för personuppgiftsansvarig samt för biträden har jag valt att återge avsnittet här.

"Nedan följer en exemplifierande beskrivning av det ansvar och skyldigheter som följer av rollerna personuppgiftsansvarig respektive personuppgiftsbiträde inom staden.

### **Den personuppgiftsansvariges ansvar**

Den personuppgiftsansvarige nämnden eller styrelsen behöver bland annat säkerställa följande.

- Personuppgiftsbehandlingen ska ha en laglig/rättslig grund. Den ska fastställas för alla befintliga behandlingar och innan en ny behandling påbörjas.
- De grundläggande principerna (artikel 5 i dataskyddsförordningen) ska implementeras i själva personuppgiftsbehandlingen av verksamheten, dvs. i verksamhetens processer.
- Om känsliga personuppgifter behandlas ska ett lagstadgat undantag från det generella förbudet för behandlingen

kunna tillämpas. Om uppgift om brott behandlas ska gällande lagstiftning iakttas.

- Den registrerade, personen vars personuppgifter behandlas, har rätt till information om den specifika behandlingen och registrerades övriga rättigheter ska beaktas.
- Inbyggt dataskydd och dataskydd som standard ska tillämpas.
- Endast anlita personuppgiftsbiträden som kan garantera att registrerades rättigheter skyddas, att tekniska och organisatoriska åtgärder som är förenliga med gällande lagstiftning implementeras, samt att personuppgiftsbiträdesavtal med instruktion, alternativt stadenintern instruktion för personuppgiftsbehandling, tecknas.
- Register över personuppgiftsbehandlingarna, registerförteckning, ska upprättas.
- Tekniska och organisatoriska skyddsåtgärder ska implementeras, upprätthålls och utvärderas enligt gällande dataskyddslagstiftning och dataskyddspraxis, ex. artikel 32 i dataskyddsförordningen.
- Personuppgiftsincidenter ska kunna upptäckas och anmälningsskyldiga personuppgiftsincidenter ska anmälas till tillsynsmyndigheten. Informationsskyldigheten gentemot den registrerade om en personuppgiftsincident ska uppfyllas.
- Konsekvensbedömning avseende dataskydd ska genomföras när så erfordras.
- Dataskyddsombud ska utnämnas.
- Tredjelandsoverföring av personuppgifter ska följa dataskyddslagstiftningens krav.

### **Personuppgiftsbitrådets ansvar**

Personuppgiftsbitrådande nämnd eller styrelse behöver bland annat säkerställa följande.

- Register över personuppgiftsbehandlingar, registerförteckning, som utförs för den personuppgiftsansvariges räkning ska upprättas.
- Medverka och säkerställa att personuppgiftsbiträdesavtal med instruktion, alternativt stadenintern instruktion för personuppgiftsbehandling, tecknas.
- Bistå personuppgiftsansvarig med anledning av begäran om utövande av den registrerades rättigheter.
- Upprätthålla och utvärdera säkerheten för personuppgiftsbehandlingen och vidta de tekniska och organisatoriska åtgärder som krävs enligt gällande dataskyddspraxis.

- Underrättelseskyldigheten gentemot den personuppgiftsansvarige, dvs. att utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident lämna lagstadgad information.
- Bistå personuppgiftsansvarig, så denne kan lämna lagstadgad information till den registrerade vid en personuppgiftsincident.
- Vid behov och begäran av personuppgiftsansvarig bistå vid utförande av konsekvensbedömning avseende dataskydd.
- Utnämna dataskyddsombud.
- Vidta åtgärder för att säkerställa laglig tredjelandsoverföring.”

Utöver dessa grundläggande krav enligt GDPR vill jag lyfta fram att det även finns skyldigheter för en personuppgiftsansvarig att informera de registrerade om de personuppgiftsbehandlingarna där den registrerades personuppgifter förekommer.

Informationen ska vara klar och tydlig och ska tillhandahållas den registrerade i god tid före det att behandlingen sker exempelvis vid insamlandet av uppgifterna eller senast inom 30 dagar från insamlandet eller om behandlingen sker dessförinnan senast vid behandlingen.

Det finns även olika krav enligt GDPR på den som utsett och anmält ett DSO till IMY, vilket gäller samtliga nämnder. Det är bland annat krav som ska säkerställa att jag som DSO ska kunna arbeta på ett oberoende sätt i verksamheten för att ha på bästa sätt kunna bevaka de registrerades friheter och rättigheter.

## Bilaga 1

### Begäran om uppgifter inför GDPR- årsrapport 2024.

Följande områden är obligatoriska att redovisa i dataskyddsombudets GDPR – Årsrapport

Då rapporten ska lämnas till respektive förvaltning vid lucia i år är tiden knapp för mig att inhämta underlag till den obligatoriska delen. Jag ber er om möjligt prioritera dessa frågor. Jag vore tacksam för att få svar inom en vecka och senast den 3 december. (Det är bra om ni svarar i vart fall övergripande. Dataskyddsarbete är en löpande process där skyddet byggs på eftersom.

Jag är tacksam för att få svar på följande frågor :

#### Registerförteckning

Då jag har tillgång till registret eller i vart fall fått en kopia av det så vet jag omfattningen av registret.

Det finns många sätt att föra register på när det gäller behandling av personuppgifter.

- Ange gärna logiken för ert register.
  - Logiken för registerförteckningen var att den baserades på den arkivstruktur som förvaltningen hade vid dataskyddslagstiftningens införande år 2018.

Register kan omfatta lagringsplatser och system, processer eller behandlingar och slutligen tjänsteleverantörer där behandlingar utförs.

- Vad omfattar ert register?
  - Omfattar våra behandlingar inom våra verksamhetsområden (processer).

Vem gör vad?

- Vem ansvarar för registerförteckningen?
  - Dataskyddsammordnare och informationssäkerhetssamordnare ska svara för praktiska hantering av personuppgiftsregistret.
- Finns det en lokal rutin kring registerföring (om Ja – var finns den)?
  - Kontrollera handlingar. Ansvarsdokument, lokal anvisning om informationssäkerhet samt arkivhanteringsrutiner .m.m
- Vem ansvarar för att processer/behandlingar registreras?

- Respektive chef svarar intern för de personuppgiftsbehandlingar som genomförs inom dess verksamhetsområde.
- Praktisk hantering DSS & ISS.
- Revideras uppgifterna i registret löpande? (Om Ja ange intervall.)
  - Nej, inga fasta intervaller beslutade i nuläget.

### Styrdokument

När det gäller styrdokument som har påverkan på dataskyddsarbetet så kan jag se två områden där det kan finnas information om hur dataskyddsarbetet är organiserat, dels i ledningssystemet och i delegations-beslut dels som en del av informationssäkerhetsarbetet.

I många organisationer finns det en tydlig avsändare på de styrdokument som bereds och antas inom en organisation. Det brukar även finnas en reglering om när ett styrdokument ska uppdateras och att det anges i dokumentet när det är gjort och även vad som ändrats så att det står klart för de berörda inom organisationen. Jag har när det gäller dataskyddsfrågorna inte hittat någon tydlig linje i de styrdokument som jag hittat. Jag vill därför få svar på följande:

- Vilka lokala styrdokument har ni antagit som rör dataskyddsfrågor (Delegationsordning, Ledningens Genomgång, lokal anvisning om informationssäkerhet etc)?
  - Delegationsordning
  - Ledningens genomgång
  - Lokal anvisning för infosäkerhetsarbete
- Är alla lokala styrdokument upplagda på nya intranätet? eller finns det styrdokument på andra platser?
  - Intranätet har vissa dokument, men finns begräsning vad som vi får publicera där avseende interna dokument. Gruppdisker för styr- och stöddokument, samt dataskydd/infosäkerhet utgör vårt bibliotek för dokument internt därav.
- Vem är ansvarig för de olika styrdokument?
  - DSS & Infosäk-samordnare för frågor
  - Olika ansvar utifrån styrdokument.

## Organisatoriska och tekniska åtgärder - Informationsklassning

Denna punkt rymmer många åtgärder men det obligatoriska området avser endast frågan om behandlingarna har informationsklassats. Om jag inte minns fel fans det en inriktning att under 2024 göra i vart fall en inventering av behandlingarna med lite högre risk gällande informationsklassning.

### Informationsklassningar

- Vem har ansvar för att det sker en informationsklassning?
  - **Genomförande infosäk.**
- Har ni gått igenom alla behandlingar som har tagits upp i registret?
  - **Det har inte under år 2024 genomförts någon omfattande kontroll eller revision av samtliga personuppgiftsbehandlingar.**
- Hur många personuppgiftsbehandlingar har informationsklassats totalt och under året?
  - **Totalt 20 st.**
  - **3 st. är infoklassats under år 2024.**
- Finns det en plan för att löpande riskbedöma behandlingarna? Om ja vad innebär den i korthet.
  - **Planen är att succesivt riskbedöma nya behandlingar och vid uppdateringar/ändringar av befintliga behandlingar. Saknar rutin för att riskbedöma äldre behandlingar.**

### Konsekvensbedömningar

Att känna till vilka behandlingar som sker eller som planeras inom en verksamhet är en viktig grundförutsättning för ett systematiskt dataskyddsarbete. En konsekvensbedömning är avsedd att lyfta fram behandlingar med högre risker i ett tidigt skede så att det finns möjlighet att ställa krav (på uppgiftsminimering, skydd, och andra åtgärder) såväl vid utveckling som inför upphandling av en tjänst eller vid en ändrad användning. Den så kallade tröskelanalysen utgår från de riskkriterier som framgår av dataskyddsförordningen samt av de riktlinjer som tillsynsmyndigheten IMY tagit fram.

- Har ni identifierat alla behandlingar med hög risk? Har ni genomfört en tröskelanalys för att se om det är nödvändigt med en konsekvensbedömning?
  - **1 st. behandling har konstaterats, konsekvensbedömning pågår (föreningsstöd- och bokningssystem).**

- Har ni genomfört de konsekvensbedömningar som har identifierats?
  - Pågående process med konsekvensbedömning av behandlingarna kopplade till föreningsstöd- och bokningssystem
- Vem är ansvarig för att det sker en tröskelanalys eller konsekvensbedömning?
  - Processägaren- ansvarig chef.
- Finns det en rutin för att uppdatera gjorda konsekvensbedömningar med viss regelbundenhet?
  - Nej, men ingår i projektet för nytt föreningsstöd- och bokningssystemet att titta över ny rutin för den behandlingen.

### Registrerades rättigheter

Denna punkt är viktig då bland annat tillsynsmyndigheten IMY har haft fokus på de registrerades rättigheter i sin tillsynsverksamhet. Det är viktigt att fånga upp begäran från registrerad i verksamheten.

- Hur många ”begäran från registrerad” (om exempelvis registerutdrag, rättelser, begränsningar m.m.) har kommit in hittills i år?
  - 1 st. begäran har inkommit år 2024. (registerutdrag)
- Hur stor andel av dessa har hanterats inom 30 dagar?
  - Ja, begäran inkom den 27/6 besvarades/hanterades den 5/7.
- Vem sköter det praktiska arbetet med begäran?
  - Registraturet hanterat förfrågningar, med stöd/vägledning från de handläggare som behövs beroende på ärendet.
- Finns det en rutin för detta arbete?
  - Ja, Instruktion för handläggning av begäran om registerutdrag avseende personuppgiften finns.

## Personuppgiftsincidenter

Jag är medveten om att det finns ett system för att anmäla in incidenter - IA. Precis som alla system så finns det vissa brister som påverkar hantering av personuppgiftsincidenter. Vid förlust av en PC eller telefon så kan den incidenten även omfatta en personuppgiftsincident. Då det endast går att styra incidenten till en kategori inom IA kan det vara så att alla personuppgiftsincidenter inte kommer att anmälas som de ska.

- Vem har ansvaret för att anmäla en personuppgiftsincident till tillsynsmyndigheten?
  - Beslut av Administrativ avdelnings chef, efter samråd med DSO
- Hur många incidenter har inträffat hittills i år?
  - Saknar sammanställning över det.
- Hur många incidenter har anmälts inom normal tid (72 timmar) från det att de var konstaterade av personuppgiftsansvarig?
  - Förvaltningen har inte anmält några PU-incidenter år 2024 till IMY ( Inga incidenter har rapporterats där det inte är osannolikt att personuppgiftsincidenten medför risk för fysiska personers fri- och rättigheter)
- Finns det någon rutin för hur incidentrapporteringen ska gå till och vem som ansvarar för vad? Var finns den i så fall?
  - Vägledning för PU-incident ligger i mappstrukturen för styrdokument, inklusive
    - \\ad.stockholm.se\cli-sd\te1sd001\SD-022448\IT telefoni och informationssäkerhet
- Följer ni upp hur incidenterna anmäls i systemet för att kunna fånga upp personuppgiftsincidenter som anmäls in som någon annan typ av incident?
  - Rutin saknas.