Stockholms stad

# GDPR Årsrapport

2021

Stockholms Stadsarkiv

**GDPR årsrapport**
Januari 2022

**Dnr:** SSA 2022/502
**Utgivningsdatum:** 2022-01-17
**Kontaktperson:** Gustav Fors

# 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:n 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 nämnden att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnden 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 nämnden ska kunna visa att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna dokumenteringsskyldighet. Årsrapporten är även ett medel för nämndens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

# Innehåll

# 2 Sammanfattning

Denna rapport är sammanställd av DSO i syfte att ge personuppgiftsansvarig (PUA), i Stadsarkivets fall är det kulturnämnden, en redogörelse för hur dataskyddsarbetet har genomförts på Stadsarkivet under 2021.

Stadsarkivet har flera viktiga delar på plats när det kommer till dataskyddsarbetet. Det finns en omfattande registerförteckning och det finns vissa mallar och stöddokumentation tillgänglig. Det saknas dock tydliga rutiner för hur arbetet med dataskydd ska ske i den löpande verksamheten. En stor brist är avsaknaden av konsekvensbedömningar där en insats bör göras under 2022 för att identifiera vilka konsekvensbedömningar som bör finnas och se till att dessa blir gjorda.

Det finns även en del organisatoriska brister där en del av det ansvar gällande dataskyddsarbete som egentligen åligger informationsägarna istället hamnar hos DSO, vilket ofta är olämpligt med tanke på att DSO:n främst ska ha en granskande roll. Ett samarbete är inlett med ett antal fackförvaltningar för att undersöka möjligheten till ett gemensamt DSO.

Sammanfattningsvis kan det konstateras att Stadsarkivet har kommit en bit på vägen med dataskyddsarbetet men att det behövs tydligare rutiner och ansvarsfördelning för att arbetet ska kunna fortgå på ett smidigt sätt och för att relevant dokumentation ska uppdateras kontinuerligt.

# 3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som 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 stadsarkivets status och DSO:ns slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:ns genomförda uppföljning och granskning.

## 3.1 Registerförteckning

### 3.1.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Antal behandlingar som är registrerade? | 148 |
| Har nödvändiga uppdateringar gjorts? | Delvis |
| Bedöms registerförteckningen vara fullständig? | Nej, den är omfattande men inte fullständig. |
| Har verksamheten lämpliga rutiner för registerföring? | Nej, lämpliga rutiner saknas. |

### 3.1.2 Syfte

I enlighet med dataskyddsförordningens artikel 30 ska stadens alla förvaltningar och bolag inventera alla personuppgifter som behandlas i verksamheten, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde, och dokumentera dem i en så kallad registerförteckning.

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 verksamhetens har lyckats inventera sina

personuppgifter och de personuppgifter som behandlas för annans räkning och upprätta en registerförteckning.

### 3.1.3 Resultat

#### Antal registrerade behandlingar

I dagsläget finns 148 personuppgiftsbehandlingar registrerade i registerförteckningen.

#### DSO kontrollerar om nödvändiga uppdateringar gjorts

Registerförteckningen uppdateras inte så ofta som är önskvärt. Små justeringar är gjorda under året men den senaste registrerade uppdateringen gjordes tidig vår 2021.

#### DSO bedömer hur fullständig registerförteckningen är

Registerförteckningen är omfattande men då den inte uppdateras regelbundet är den inte fullständig. Vissa behandlingar saknas helt och vissa behandlingar saknar en angiven informationsägare.

#### DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Det saknas tydliga rutiner för hur, när och av vem registerförteckningen ska uppdateras. I dagsläget tycks uppdateringar ske främst på uppmaning från DSO. Den instruktion om hur förteckningen ska fyllas i som finns är inte användarvänlig.

### 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 |
| 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 den nuvarande registerförteckningen är svåröverskådlig och det inte finns några fastställda rutiner för hur uppdateringar av registret ska ske är det troligt att det saknas en del personuppgiftsbehandlingar i systemet och att det inte uppdateras så frekvent som det borde. Den befintliga förteckningen är dock omfattande och det är DSO:s uppfattning att de flesta behandlingar finns med i förteckningen.

### 3.1.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att registerförteckningen under 2022 överförs från dagens Word-fil till det av staden upphandlade och rekommenderade systemet DraftIT Privacy Records. Systemet ger en bättre överblick och gör det enklare att uppdatera förteckningen vilket bör bidra till att uppdateringar görs mer löpande vartefter nya eller förändrade personuppgiftsbehandlingar införs i verksamheten.

I samband med övergången till DraftIT Privacy Records bör en omfattande genomgång göras av förteckningen och nya rutiner för hur uppdateringar av förteckningen ska ske tas fram. Stadsarkivet har en licens till systemet och det är redo att användas.

Ansvariga för att hålla registerförteckningen uppdaterad är informationsägarna, oftast avdelningscheferna, men även processledare bör medverka både vid uppdateringen av förteckningen och vid framtagandet av rutiner då dessa har god insyn i vilka behandlingar som finns i verksamheten och på vilket sätt de sker.

## 3.2 Styrdokument

### 3.2.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Finns lämplig styrande dokumentation på plats? | Ja |
| Håller innehållet i de existerande dokumenten lämplig kvalitet? | Nej |
| Är dokumenten pedagogiska och ger de ett tillräckligt stöd? | Nej |
| Är dokumenten uppdaterade? | Delvis |
| Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov? | Nej, ansvaret ligger till stor del på DSO. |

### 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 de styrdokument antagna och på plats, dels ska rapporteringen visa om dokumentationen innehållsmässigt håller en lämplig kvalitet, i vilket ingår bl.a. 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.

### 3.2.3 Resultat

#### Finns lämplig styrande dokumentation på plats?

Stadsarkivet har de styrande dokument på plats som dataskyddsförordningen föreskriver och som Stadsledningskontoret (SLK) uppmanar till.
I en del fall finns centrala dokument och mallar framtagna av SLK, dessa har i viss mån anpassats till Stadsarkivets verksamhet.
De styrdokument och mallar som finns är samlade och tillgängliga för Stadsarkivets medarbetare i en gemensam katalog.
Sedan 2020 finns Stadsarkivets dataskyddsorganisation fastställd i beslut av Förvaltningschefen.

#### DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

De flesta dokumenten behöver uppdateras och anpassas bättre till Stadsarkivets verksamhet.

### 3.2.4 DSO anger hur allvarliga bristerna är på en skala

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

Dokumentation finns men den är inte helt uppdaterad och anpassad till Stadsarkivets verksamhet. Det finns också vissa frågetecken kring hur kännedomen kring dessa styrdokument är i organisationen.

Den dataskyddsorganisation som finns fastställd behöver uppdateras och vidareutvecklas för att kunna användas praktiskt i verksamheten.

### 3.2.5 DSO ger råd och rekommendationer till PUA

En översyn av nuvarande dokumentation bör göras av de som enligt den fastställda dataskyddsorganisationen har användning av dokumenten i samråd med DSO. Nämnda dataskyddsorganisation behöver uppdateras så att den går att tillämpa i praktiken och information om vad den innebär när det kommer till ansvarsfördelning i dataskyddsarbetet behöver spridas i organisationen.

## 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? | 19 |
| Är klassade personuppgiftsbehandlingar aktuella? | Delvis |

### 3.3.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd så 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 faktisk 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.

### 3.3.3 Resultat

Av de 19 informationsklassningar som gjorts är det två, eDok systemstöd och e-arkiv Stockholm, som är fullständiga. Övriga informationsklassningar har endast klassats utifrån ett dataskyddsperspektiv. Dessa 17 informationsklassningar gjordes våren 2019 och behöver ses över igen. Klassningarna avseende eDok systemstöd och e-arkiv Stockholm gjordes hösten 2021 och är uppdaterade.

### 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 |
| 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 |

En stor del av DSO:s fokus under 2021 har varit att se till informationsklassningar av e-arkiv Stockholm och eDok systemstöd kommit på plats. Vid granskning utförd av revisionskontoret under juni 2019 framkom bland annat att Stadsarkivet inte hade gjort informationsklassningar avseende e-arkiv Stockholm och eDok systemstöd. Dessa brister har nu till sist åtgärdats men det kvarstår arbete med att se över och identifiera ytterligare informationstillgångar som behöver klassas. Exempelvis måste Stadsarkivets eget användande av eDok klassas. De informationsklassningar som gjordes våren 2019 och behöver ses över igen.

### 3.3.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att en genomgång av de befintliga informationsklassningarna från 2019 görs av respektive informationsägare i samråd med DSO avseende personuppgiftsbehandlingen och med hjälp av informationssäkerhetssamordnare för att utreda om ytterligare

klassning ur ett informationssäkerhetsperspektiv behövs för dessa behandlingar.

I samband med uppdateringen av registerförteckningen bör tillfälle ges att identifiera ytterligare behandlingar som ska klassas. DSO rekommenderar att en genomgång av detta görs i samband med översynen av registerförteckningen.

Vidare är det DSO:s starka rekommendation att det Stadsarkivets egen information i eDok klassas under 2022. Ansvariga för detta arbete är utsedda och DSO och informationssäkerhetssamordnare finns tillgängliga för stöd.

## 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? | Nej |

### 3.4.2 Syfte

Konsekvensbedömningen hjälper organisationen att identifiera och minimera integritetsriskerna för personuppgifter som behandlas i verksamheten. 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 eller 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 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, ingen övergripande genomgång har gjorts för att identifiera om det finns fler behandlingar som behöver konsekvensbedömmas,

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Nej, en utredning kring vilka potentiella högriskbehandlingar av personuppgifter som kan förekomma i verksamheten behövs. Vid en genomgång av det aktuella personuppgiftsregistret tycks det dock inte finnas några pågående behandlingar som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter enligt artikel 35.1.

Är de genomförda konsekvensbedömningarna aktuella?

De bedömningar som gjorts har gjorts inför tillfälliga behandlingar så som tekniska tester av system och dylikt. De är därför inte längre aktuella.

### 3.4.4 DSO anger hur allvarliga bristerna är på en skala

| | |
|---|---|
| x | 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 |

Avsaknaden av konsekvensbedömningar och riskanalyser är en allvarlig brist i Stadsarkivets dataskyddsarbete. Då konsekvensbedömningar är ett krav för vissa personuppgiftsbehandlingar och även i övrigt är ett bra verktyg för att identifiera vilka risker en viss personuppgiftsbehandling kan medföra för de registrerade är det av högsta vikt att en ordentlig översyn görs på detta område.

### 3.4.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar starkt är att en ordentlig översyn av pågående personuppgiftsbehandlingar görs för att identifiera för vilka behandlingar det bör göras konsekvensbedömningar. Förslagsvis görs denna översyn i samband med uppdateringen av registerförteckningen.

Ansvaret för denna översyn ligger främst på informationsägarna, vilket i de flesta fall är avdelningscheferna.

I likhet med flera övriga områden rekommenderas att tydliga rutiner för när, hur och av vem konsekvensbedömningar ska göras. Dessa rutiner bör tas fram av informationsägarna i samråd med DSO.

## 3.5 Individens rättigheter

### 3.5.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer? | En begäran om radering och en begäran om komplettering har inkommit. |
| Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar? | Båda hanterades inom en vecka. |

### 3.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen 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 personuppgiftsansvarig 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 begära rättning av vissa uppgifter.

Verksamheten har enligt dataskyddsförordningen en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran.

### 3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

DSO bedömer att verksamheten har mycket goda förutsättningar att hantera registrerades rättigheter i tid.

Under året har en begäran om radering av personuppgifter och en begäran om komplettering av personuppgifter inkommit till Stadsarkivet, båda rörde arkivhandlingar. Stadsarkivet besvarade dessa inom en vecka i enlighet med gällande lagstiftning.

### 3.5.4 DSO anger hur allvarliga bristerna är på en skala

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

### 3.5.5 DSO ger råd och rekommendationer till PUA

De begäran som inkommit från registrerade personer har behandlas snabbt och korrekt av Stadsarkivet. Den enda synpunkt DSO har är att, vilket sammanfaller med det som nämnts ovan i avsnitt 3.2, den dokumentation som finns gällande de registrerades rättigheter kan behöva ses över. Detta som ett led i att få till tydligare och mindre personberoende rutiner.

## 3.6 Personuppgiftsincidenter

### 3.6.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Hur upptäcks personuppgiftsincidenter? | Av medarbetare som rapporterar till DSO. |
| Hur många personuppgiftsincidenter har dokumenterats? | En. |
| Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte? | En har rapporterats till IMY. |
| Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten? | Den som rapporterades skickades in i tid. |

### 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 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:s sida. 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

Hur väl förmår verksamheten att rapportera personuppgiftsincidenter i tid till Integritetsskyddsmyndigheten?

De incidenter som upptäcks och dokumenteras rapporteras till IMY inom de föreskrivna 72 timmarna.

### 3.6.4 DSO anger hur allvarliga bristerna är på en skala

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

Det finns goda rutiner för rapportering av incidenter och IMY underrättas inom föreskriven tid när så krävs. Dock är det väldigt få incidenter som rapporteras. Det är därför troligt att incidenter som av medarbetare uppfattas som mindre allvarliga inte rapporteras.

### 3.6.5 DSO ger råd och rekommendationer till PUA

Vidare utbildning av medarbetare och kommunikation kring vikten av att rapportera alla personuppgiftsincidenter oavsett hur allvarliga de tycks vara behövs. Ansvar för detta ligger på DSO i samråd med avdelningschefer och processledare.

# 4 Genomförda granskningar under året

## 4.1 Sammanfattning

Nuvarande DSO tillträdde i mars 2021. Fokus har under året legat på att granska hur Stadsarkivets dataskyddsarbete fungerat hittills på ett övergripande plan. Denna årsrapport kan därför ses som resultatet av DSO:s granskningar under året. Dessutom har uppföljningar gjorts av tidigare granskningar av eDok, e-arkiv Stockholm och personalområdet. Förutom de områden som redan tagits upp i denna rapport har en genomgång av Stadsarkivets personuppgiftsbiträdesavtal gjorts.

## 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

### 4.3.1 Personuppgiftsbiträdesavtal

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

Förutom de områden som redan tagits upp i denna rapport har en genomgång av Stadsarkivets personuppgiftsbiträdesavtal (PUB-avtal) gjorts av DSO. Stadsarkivet har PUB-avtal på plats för de personuppgiftsbehandlingar som kräver det. En del av dessa avtal börjar dock bli ganska gamla och bör ses över.

## 4.4 DSO ger råd och rekommendationer till PUA

Ansvariga för de befintliga PUB-avtalen, oftast avdelningschefer, bör gå igenom dem för att se om de behöver uppdateras.

# 5 Risker inom dataskydd

## 5.1 Sammanfattning

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

## 5.2 Syfte

Verksamheten har ansvar för att göra vissa typer av riskanalyser, så som konsekvensbedömningar och informationsklassningar, men dessa ger inte en heltäckande bild av personuppgiftsriskerna i verksamheten. Dataskyddsombudet behöver som underlag för sin egen planering och sitt löpande arbete ha kontinuerlig överblick över dessa risker, i verksamhetens samtliga personuppgiftsbehandlingar. Exempelvis krävs en sådan överblick för att kunna välja ut vilka områden som bör granskas under det kommande året eller för att avgöra vilka råd som dataskyddsombudet behöver lämna till verksamheten om dataskyddsåtgärder som behöver vidtas.

## 5.3 Resultatet av riskkartläggningen

Som tidigare nämnts finns det på Stadsarkivet inom de flesta delar av dataskyddsområdet en bra grund att arbeta vidare från. Genomgående saknas det dock tydliga instruktioner, rutiner och ansvarsfördelningar. En dataskyddsorganisation för Stadsarkivet fastställdes hösten 2020. I denna finns olika ansvarsområden fördelade men hittills har den inte följts. Denna fastställda organisation behöver också ses över så ansvarsområdena är fördelade på ett korrekt och rimligt sätt. I dagsläget ligger mycket av ansvaret på dataskyddsområdet som helhet hos DSO, som behöver påminna och informera om vilka åtgärder som behöver göras. För att få ett fullt fungerande dataskyddsarbete behöver dessa frågor integreras i den dagliga verksamheten och skötas löpande av såväl chefer som medarbetare, beroende vilka frågor det rör sig om. Först då kommer dataskyddsarbetet att kontinuerligt uppdateras och fungera i praktiken.

Risken med nuvarande ordning är att dataskyddsarbetet riskerar att bli eftersatt eftersom det idag i många delar är personberoende och fristående från den ordinarie verksamheten. Dataskyddsarbetet bör bli en naturlig del av det löpande arbetet vilket också skulle leda till att dataskyddsfrågor inte känns lika främmande och svårhanterliga som det upplevs som att de på många håll i verksamheten gör idag.

## 5.4 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att ledningsgruppen inleder ett arbete med att se över dataskyddsorganisationen och aktivt arbetar tillsammans med DSO för att integrera dataskyddsarbetet mer i verksamheten. Detta kräver också ytterligare utbildningsinsatser, vilket är avdelningschefernas ansvar tillsammans med DSO.

# 6 Planerade granskningar under det nya verksamhetsåret

## 6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Ekonomi
- Registerförteckning och Konsekvensbedömningar
- Pedagogiska verksamheten

## 6.2 Syfte

Som nämnts ovan är det granskande arbetet en av dataskyddsombudets viktigaste uppgifter. Eftersom dataskyddsombudet ofta har begränsat med tid, behöver granskningsplanen för det nya året utformas med eftertanke. Som en tumregel bör två-tre granskningar ses som en rimlig granskningsinsats under ett verksamhetsår. Granskningsområdena bör lämpligen väljas utifrån ett riskbaserat synsätt, det vill säga att fokus bör ligga på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Därigenom åstadkoms en röd tråd i dataskyddsarbetet från ett verksamhetsår till nästa samtidigt som de största riskerna elimineras eller åtminstone sänks till en mer acceptabel nivå.

## 6.3 Planerade granskningar

### Ekonomi

En granskning av personuppgiftsbehandling inom området ekonomi var planerad till 2021 men fick skjutas upp till 2022 då uppföljning av tidigare granskningar visade sig tidskrävande.

### Registerförteckning och konsekvensbedömningar

Under sista kvartalet 2022 kommer en större granskning och genomgång av registerförteckning och konsekvensbedömningar att göras för att se om de brister som beskrivits i denna rapport har åtgärdats. DSO kommer naturligtvis även att ha en rådgivande funktion under arbetet med att åtgärda bristerna.

### Pedagogiska verksamheten

Då den pågående pandemin har lett till att mycket av den pedagogiska verksamheten i form av visningar och föredrag har övergått till att ske digitalt finns det anledning att granska hur personuppgifter behandlas i den verksamheten.

# 7 Övrigt att rapportera

## 7.1 Sammanfattning

Ett samarbete har inletts med fem andra fackförvaltningar för att se över möjligheten att ha ett gemensamt DSO.

## 7.2 Syfte

Avsikten med denna punkt i årsrapportmallen är att ge möjlighet att komplettera bilden av statusen i dataskyddsarbetet. Under denna rubrik kan 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.

## 7.3 Övriga observationer

### Gemensamt DSO

Tillsammans med fem andra fackförvaltningar utreds möjligheterna att ha ett gemensamt DSO. Detta dels som ett led i ett utökat samarbete mellan förvaltningarna och dels då det finns fördelar med ett DSO som arbetar heltid med dataskyddsfrågor och som är mer självständig gentemot verksamheterna än ett DSO som är anställd av förvaltningen.

Formen för detta samarbete är inte fastställd men diskussioner pågår för att få till en lösning under 2022.

## 7.4 DSO ger råd och rekommendationer till PUA

DSO:s rekommendation är att Stadsarkivet går vidare med samarbetet och att ett gemensamt DSO som kan arbeta heltid med dataskyddsfrågor tillsätts.