Stockholms stad

Bilaga 4

GDPR Årsrapport

År 2025

Stadsarkivet

GDPR årsrapport
Januari 2026

Dnr: SSA 2026/150
Utgivningsdatum: 2026-01-16
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 nämnd och styrelse 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 nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

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

Innehåll

2 Sammanfattning

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. Det leder till brister i det systematiska dataskyddsarbetet. 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.

DSO bedömer dock att Stadsarkivet har bättre förutsättningar nu än tidigare att omhänderta de brister som finns på området.

En större personuppgiftsincident drabbade Stockholms stad under 2025 vilket ger anledning till att Stadsarkivet bör göra en översyn över hur personuppgifter tillhörande anställda inom förvaltningen behandlas av övriga verksamheter i staden och om nödvändiga åtgärder har vidtagits inom ramen för detta.

3 Obligatoriska rapporteringsområden

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

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

Nedan redogörs för nämndens eller bolagets status och DSO: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
Har verksamheten lämpliga rutiner för registerföring?	Nej

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

DSO kontrollerar hur många behandlingar som registrerats

[Text]

DSO kontrollerar om nödvändiga uppdateringar gjorts

Uppdateringar görs delvis, men är personberoende. Tydliga rutiner för uppföljning saknas

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.

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 det saknas tydliga rutiner för när, hur och av vem personuppgiftsregistret ska uppdateras skiljer det sig åt mellan Stadsarkivets olika verksamhetsgrenar hur ofta nya behandlingar läggs till i förteckningen och när tidigare behandlingar uppdateras. Den befintliga förteckningen är dock omfattande och det är DSO:s uppfattning att de flesta behandlingar finns med i företeckningen. Om rutiner för uppdatering inte tas fram riskerar registerförtekningen att bli daterad och ofullständig, vilket innebär

att den inte lever upp till kraven som ställs i dataskyddsförordningen.

3.1.5 DSO ger råd och rekommendationer till PUA

För att säkerställa att registerförteckningen uppdateras regelbundet behöver det fastställas vem som har det övergripande ansvaret att samordna arbetet med registerförteckningen och ta fram lämpliga rutiner i samråd med exempelvis DSO och ämbetsarkivarie. DSO rekommenderar att detta samordningsansvar ska tilldelas Stadsarkivets dokumentcontroller.

3.2 Styrdokument

3.2.1 Sammanfattning

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

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.

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?

Stadsarkivet har de flesta av de styrande dokument som dataskyddsförordningen föreskriver och som Stadsledningskontoret (SLK) uppmanar till på plats. 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.

En lokal anvisning för informationssäkerhet saknas. En sådan lokal anvisning redogöra för hur stadens övergripande ledningssystem för informationssäkerhet omhändertas i den egna verksamheten. I detta ingår även att beskriva ansvarsfördelningen för dataskyddsarbetet inom förvaltningen, så väl det operativa som det granskande och stödjande.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

Merparten av existerande dokumentation behöver ses över och troligen uppdateras för att anpassas till Stadsarkivets nuvarande organisation.

3.2.4 DSO anger hur allvarliga bristerna är på en skala

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

Dokumentation finns men den är inte alltid uppdaterad och anpassad till Stadsarkivets nuvarande organisation. Det finns också vissa frågetecken kring hur kännedomen kring dessa styrdokument är i organisationen. En lokal anvisning för informationssäkerhet saknas och i och med det även en dokumenterad ansvarsfördelning avseende dataskyddsarbetet. Det innebär att det finns en otydlighet

kring var ansvaret för det operativa dataskyddsarbetet ligger vilket riskerar att leda till att nödvändiga åtgärder uteblir. Viss ny styrdokumentation har dock tillkommit avseende enheten IT och Digitalisering vilket är positivt.

3.2.5 DSO ger råd och rekommendationer till PUA

Befintlig dokumentation behöver ses över och vid behov uppdateras. En fastställd ansvarsfördelning avseende dataskyddsarbetet bör tas fram, förslagsvis till att börja med som en del av den lokala anvisningen för informationssäkerhet.

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?	6
Är klassade personuppgiftsbehandlingar aktuella?	Ja

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 av, 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

Arbetet med att informationsklassa Stadsarkivets informationstillgångar går framåt. Under året har bland annat Stadsarkivets egen information i eDok informationsklassats. Det kvarstår ett arbete med att informationsklassa alla informationstillgångar som innehåller personuppgifter men DSO:s bedömning är att förutsättningarna för att Stadsarkivet ska genomföra nödvändiga informationsklassningar är bättre än tidigare.

3.3.4 DSO anger hur allvarliga bristerna är på en skala

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

3.3.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att informationstillgångar innehållandes personuppgifter prioriteras i arbetet med informationsklassningar. Övriga rekommendationer angående informationsklassningar ges av informationssäkerhetssamordnare i Ledningens genomgång av informationssäkerhet.

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?	Ja

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 fullständig genomgång av vilka behandlingar som behöver konsekvensbedömmas har gjorts. En inventering av vilka av Stadsarkivets register och databaser som innehåller personuppgifter har dock påbörjats.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Konsekvensbedömning har under 2025 gjorts för den behandling som enligt bedömning sannolikt kunnat leda till en hög risk för fysiska personers rättigheter och friheter. Behandling är ett led i Stadsarkivets arbete med att tillgängliggöra skolbetyg via en webtjänst.

Det kan dock finnas fler högriskbehandlingar där konsekvensbedömning ej genomförts, i och med att ingen fullständig genomgång av vilka behandlingar som bör konsekvensbedömmas har gjorts.

Är de genomförda konsekvensbedömningarna aktuella?

Ja, men sannolikt bör fler bedömningar genomföras.

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

Bristerna avseende konsekvensbedömningar kvarstår i stort från tidigare år. En viss förbättring har skett då konsekvensbedömning avseende en högriskbehandling har gjorts i enlighet med dataskyddsförordningens regler. Det saknas dock fortfarande tydliga rutiner för när och hur konsekvensbedömningar ska genomföras. DSO rekommenderar att resurser avsätts för att göra en genomlysning av Stadsarkivets personuppgiftsbehandlingar för att i första hand identifiera potentiella högriskbehandlingar där konsekvensbedömning ska genomföras enligt dataskyddsförordningen.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	3
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	Samtliga

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. I regel gäller de begäran om rättelse, radering etc. som Stadsarkivet får in ändring av personuppgifter i arkivhandlingar. När det gäller personuppgifter i arkiverade handlingar hos en arkivmyndighet finns det undantag från dessa rättigheter i arkivförordningen (1991:446) vilket innebär att Stadsarkivet inte har någon skyldighet att exempelvis rätta

personuppgifter i arkivhandlingarna. Begäran ska ändå besvaras inom de stadgade 30 dagar, vilket Stadsarkivet har goda rutiner för.

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 behandlats 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?	1
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	1
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Samtliga

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.

3.6.3 Resultat

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

För de incidenter som upptäcks och dokumenteras görs en bedömning av om rapportering till IMY behöver ske och eventuell rapportering görs 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
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	Inga brister av nämnvärd betydelse identifierade

De incidenter som rapporteras behandlas inom föreskriven tid. 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

Utbildning av medarbetare och kommunikation kring vikten av att rapportera alla personuppgiftsincidenter oavsett hur allvarliga de tycks vara behövs.

Den incident som anmälts till IMY var den stadsövergripande incidenten som skedde i företaget Miljödatas system. Denna incident föranleder ett behov av att utreda hur personuppgiftsansvaret är reglerat mellan stadens nämnder. DSO rekommenderar att detta följs upp. Se mer under avsnitt 7 ”Övrigt att rapportera”.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Personuppgiftsbiträdesavtal

4.2 Syfte

DSO ska i sitt arbete göra återkommande granskningar av hur väl GDPR efterlevs i verksamheten. Resultaten av granskningarna ligger sedan till grund för vilka beslut verksamheten fattar 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 resultatet av granskningarna.

4.3 Genomförda granskningar och deras resultat

Personuppgiftsbiträdesavtal

	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 granskning av Stadsarkivets personuppgiftsbiträdesavtal visar att det finns vissa brister både vad gäller kvaliteten och förekomsten avseende personuppgiftsbiträdesavtal.

4.4 DSO ger råd och rekommendationer till PUA

En översyn bör göras dels av Stadsarkivets befintliga personuppgiftsbiträdesavtal men också en inventering av var det i nuläget saknas avtal. Både vad gäller de fall där Kulturnämnden

genom Stadsarkivet är personuppgiftsansvarig och där den är personuppgiftsbiträde. En uppdatering pågår av de personuppgiftsbiträdesavtal som Stadsarkivet tecknar med andra bolag och nämnder inom staden i samband med de arkivtjänster Stadsarkivet erbjuder.

Motsvarande översyn bör göras avseende behovet av personuppgiftsbiträdesavtal mellan Stadsarkivet och stadens verksamheter när det gäller förvaltningen av det stadsgemensamma ärendehanteringssystemet eDok. En sådan översyn är dock beroende av hur staden centralt ser på de behandlingar som sker i stadens gemensamma centrala system.

Stadsarkivets samverkan med Riksarkivet och användandet av arkivredovisningssystemet Arkis behöver också utredas avseende personuppgiftsansvaret.

5 Risker inom dataskydd

5.1 Sammanfattning

Den största risken inom dataskydd för Stadsarkivet är att 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. För att komma till rätta med detta behöver en tydlig organisation för dataskydds- och informationssäkerhetsarbetet finnas på plats. DSO:s roll behöver renodlas till en granskande och rådgivande funktion så det faktiska dataskyddsarbetet kan pågå integrerat i verksamheterna.

Förutsättningarna för att få till en fungerande dataskyddsorganisation är bättre än tidigare på Stadsarkivet. Dels på grund av att omorganisationen lett till en tydligare ansvarsfördelning avseende Stadsarkivets IT och dels då en dokumentcontroller med ansvar för att ta fram rutiner för Stadsarkivets informationshantering har anställts.

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. DSO 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 DSO behöver lämna till verksamheten om dataskyddsåtgärder som behöver vidtas.

5.3 Resultatet av riskkartläggningen

Risken med att Stadsarkivets dataskyddsarbete är personberoende och inte en integrerad del av den löpande verksamheten med tydliga rutiner är kvarstående från tidigare år. DSO är medveten om att det för en mindre organisation finns svårigheter med att avsätta nödvändiga resurser för att prioritera dataskyddsarbetet. Men bedömningen är att det finns bättre förutsättningar nu än tidigare för att genomföra vissa insatser för att förbättra det löpande dataskyddsarbetet.

Stadsarkivets omorganisation har lett till att ansvaret för Stadsarkivets IT-system har samlats i en enhet där erfarenhet finns sedan tidigare avseende informationssäkerhets- och dataskyddsarbete som ett led i förvaltningen av eDok. De rutiner och lathundar som finns på plats för enheten IT och digitalisering kan användas för att ta fram rutiner som är övergripande för hela Stadsarkivet.

En dokumentcontroller med ansvar för att ta fram rutiner avseende Stadsarkivets informationshantering har anställts. Denna nya funktion ger också förutsättningar för att ta fram och implementera rutiner avseende dataskyddsarbetet.

5.4 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att de förbättrade förutsättningarna för att utveckla dataskyddsarbetet tas tillvara på under 2026 så att rutiner och riktlinjer kommer på plats och blir kända i organisationen.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Stadsarkivets publicerade information*
- *Stadsarkivets sociala medier och andra externa kommunikationskanaler*

Samt uppföljning av personuppgiftsbiträdesavtal.

6.2 Syfte

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

Stadsarkivets publicerade information

En granskning av den information som Stadsarkivet har publicerat i externa kanaler och huruvida den innehåller personuppgifter och om nödvändiga åtgärder i sådana fall har vidtagits. I och med att informationen gjorts tillgänglig för allmänheten är det av särskild vikt att personuppgiftsbehandlingen det kan innebära sker i enlighet med dataskyddsförordningens regler.

Stadsarkivets sociala medier och externa kommunikationskanaler

Likt Stadsarkivets publicerade information vänder sig Stadsarkivets användande av sociala medier och andra externa kommunikationskanaler till allmänheten. Det finns också anledning

att granska de eventuella tredjelandsöverföringar som kan ske i samband med detta.

7 Övrigt att rapportera

Under 2025 drabbades staden av en större personuppgiftsincident där uppgifter om anställda röjdes. Incidenten skedde i form av ett antagonistiskt angrepp, en så kallad ransomware-attack, mot leverantören Miljödatas IT-miljöer. Uppgifter om stadens anställda fanns i en version av arbetsmiljösystemet Stella som ännu inte tagits i drift. Personuppgifterna hade överlämnats till Miljödata från enheten för hr-system vid Stadsledningskontoret.

Incidenten väcker frågor kring hur Stockholms stad ser på personuppgiftsansvaret när personuppgifter avseende anställda vid en förvaltning behandlas av en annan nämnd, exempelvis när det gäller stadsgemensamma centrala system.
I det aktuella fallet uppmanades alla förvaltningar att göra en egen incidenthantering trots att incidenten i realiteten varit skett med i en personuppgiftsbehandling som Stadsledningskontoret ansvarat för och att personuppgiftsbiträdesinstruktion mellan Stadsledningskontoret och övriga nämnder saknats avseende denna behandling.

En central översyn av personuppgiftsansvaret för dessa typer av behandlingar ska göras av Stadsledningskontoret.

DSO rekommenderar att denna översyn följs upp och att Stadsarkivet ser över vilka personuppgifter för anställda som behandlas av andra aktörer inom staden. Översynen kan också få påverkan för vilka krav som ställs på Stadsarkivets behandling av andra verksamheter i stadens personuppgifter inom förvaltningen av det stadsgemensamma systemet eDok.