Stockholms stad

GDPR Årsrapport

År 2024

Stadsarkivet

GDPR årsrapport
Januari 2025

Dnr: SSA 2025/213
Utgivningsdatum: 2025-01-17
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 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

I egenskap av ert DSO lämnar jag följande årsrapport.

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.

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 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

I dagsläget finns 148 personuppgiftsbehandlingar registrerade i registerförteckningen.

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. I dagsläget tycks uppdateringar ske främst på uppmaning från DSO.

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

Under 2025 behöver färdigställandet av registerförteckningen att prioriteras då denna är en viktig grund för det fortsatta dataskyddsarbetet.

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 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.

Den sedan 2020 fastställda dataskyddsorganisationen för Stadsarkivet är efter Stadsarkivets omorganisation inte längre tillämplig.

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 är inte relevant efter Stadsarkivets omorganisation under 2024.

3.2.5 DSO ger råd och rekommendationer till PUA

En översyn av nuvarande dokumentation bör göras.
Då den fastställda dataskyddsorganisationen inte är tillämplig längre behöver ansvar och arbetsfördelning avseende dataskyddsfrågor fastställas på nytt under 2025.

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?	3
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

Som lyfts i tidigare årsrapporter är Stadsarkivets informationstunga system eDok och e-arkiv Stockholm kontinuerligt informationsklassade. Under 2024 har även en del av Stadsarkivets lokala system informationsklassats i samband med att de ska överföras till systemtjänsteavtalet. Men det finns fortfarande informationstillgångar som inte har informationsklassats. Bland annat behöver Stadsarkivets eget användande av eDok klassas.

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

En insats behöver göras under 2025 för att klassa de informationstillgångar som ännu inte klassats.

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 fullständig genomgång av vilka behandlingar som behöver konsekvensbedömmas har gjorts.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Nej.

Är de genomförda konsekvensbedömningarna aktuella?

De bedömningar som gjorts tidigare 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.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	2
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.

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?	1
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer)?	0
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	-

3.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskyddsförordningen (artikel 4.12) ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller

till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.”

I en verksamhet kan 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.

4 Genomförda granskningar under året

4.1 Sammanfattning

Av resursbrist och byte av DSO har inga granskningar genomförts under 2024. Detta är naturligtvis en brist som behöver ses över och som hänger ihop med att DSO:s roll behöver renodlas till en granskande och rådgivande funktion.

5 Risker inom dataskydd

5.1 Sammanfattning

De största riskerna 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.

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

Stadsarkivet har inom de flesta delar av dataskyddsområdet en bra grund att arbeta vidare från. Genomgående saknas det dock tydliga instruktioner, rutiner och ansvarsfördelningar. En dataskydds-organisation för Stadsarkivet fastställdes hösten 2020. Denna implementerades aldrig ordentligt och i och med Stadsarkivets omorganisation är den nu obsolet. 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.

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 enhetschefernas ansvar tillsammans med DSO.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Kommunikation
- Registerförteckning och Konsekvensbedömningar

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

Kommunikation

Kommunikationsområdet är en personuppgiftstung verksamhet där användandet av sociala medier och andra kanaler spelar en stor roll. Det är också ett område där insynen är stor vilket gör det extra viktigt att det finns ordentliga rutiner för hur personuppgifter får behandlas.

Registerförteckning och konsekvensbedömningar

En större uppföljning av arbetet med registerförteckning och konsekvensbedömningar kommer med anledning av resultatet i denna årsrapport att genomföras under året.

7 Övrigt att rapportera

Som framkommit i rapporten är en central del i Stadsarkivets kommande dataskyddsarbete att tydliggöra roller och ansvar i dessa frågor. Som ett led i detta har det beslutats att en dokumentcontroller ska anställas som bland annat kommer att ha ett samordnande ansvar för dataskyddsarbetet.
DSO framhåller att detta är ett mycket bra beslut och rekommenderar att en ny dataskyddsorganisation tas fram när denna tjänst är tillsatt.