Stockholms stad

Bilaga 11

GDPR Årsrapport

År 2024

Skarpnäcks stadsdelsförvaltning

GDPR årsrapport
Januari 2025

Dnr: SKA 2024/775
Utgivningsdatum: 2025-01-30
Kontaktperson: Amanda Johansson, dataskyddsombud

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 Dataskyddsombud lämnar vi följande årsrapport.

Dataskyddsarbetet i förvaltningen har under året stärkts på flera håll jämfört med föregående år. Registerförteckningen är idag mer omfattande än tidigare och reflekterar på ett bättre sätt de personuppgiftsbehandlingar som sker runtom i förvaltningen. Arbetet med att identifiera, kartlägga och vidta åtgärder gällande högriskbehandlingar behöver alltjämt stärkas och bör därför prioriteras under nästkommande år. En del av detta arbete kan ske i samband med informationsklassningar, men dataskyddsförordningens särskilda krav på konsekvensbedömningar vid högriskbehandlingar behöver beaktas.

Det granskande arbetet har utgått från dataskyddsombudets årshjul samt de prioriteringar av granskningar som planerades i 2023 års rapport. Exempelvis visade granskningen av efterlevnaden av den nya rutinen för personuppgiftsincidenter på fortsatt behov av att stärka kunskaperna om de krav som dataskyddsförordningen ställer på dokumentation av incidenter.

Registerförteckningen är den delen av dataskyddsarbetet som tydligast förbättrats med nya registreringar och kontrollerade äldre registreringar. Vid genomgång av registerförteckningen har ett behov av kunskapsstärkande insatser identifierats vilket bör prioriteras under kommande år.

Vad gäller de tekniska och organisatoriska åtgärderna för personuppgiftsbehandlingar bedöms avsaknaden av fler genomförda informationsklassningar utgöra en omfattande brist. Det har däremot skett en förbättring jämfört med förra årets bedömning. Det finns idag en tydligare plan än tidigare för klassningsarbetet och flera lokala klassningar har påbörjats. Eftersom fastställda lokala klassningar alltjämt saknas 2024 får bristen anses vara omfattande till dess att klassningar genomförts i större antal och i sin helhet.

Denna rapport är skriven av Julia Ögren och Amanda Johansson, dataskyddsombud.

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?	158
Har nödvändiga uppdateringar gjorts?	Nej
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

Det följer i klartext av artikel 30 dataskyddsförordningen att stadens alla förvaltningar och bolag måste inventera alla personuppgifter som

behandlas i verksamheten, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde, och dokumentera dem i en så kallad registerförteckning (även kallat behandlingsregister).

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

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

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

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

I dagsläget finns 158 behandlingar registrerade i registerförteckningen.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Sedan augusti i år har majoriteten av befintliga registreringar uppdaterats i någon mån vilket är en stor förbättring sedan tidigare år, många har därtill tillkommit. Vad gäller kvalitén på innehållet i registreringarna behöver den stärkas och återkoppling har skickats från dataskyddsombudet till ansvariga chefer för att följa upp vissa frågeställningar och öka tydligheten i beskrivningar och bedömningar. Ett antal registreringar är också enbart påbörjade och innehåller i dagsläget mycket sparsamt med information. I sin helhet kan det därmed inte sägas att nödvändiga uppdateringar gjorts eftersom dataskyddsförordningen ställer specifika krav på innehållet.

DSO bedömer hur fullständig registerförteckningen är

Registerförteckningen innehåller idag registreringar från alla avdelningar, men bedöms inte vara fullständig eftersom vissa verksamheter ännu helt saknar registreringar och samtliga personuppgiftsbehandlingar som sker inom ramen för avdelningarna har inte registrerats. Vissa nya registreringar har påbörjats men saknar viktiga delar för att anses tillräckligt beskrivna. Sammanfattningsvis är registerförteckningen därför inte att anse som fullständig, men förvaltningen tar tydliga steg framåt i arbetet.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Rutinen gällande registrering och uppdatering av registerförteckningen togs fram under 2023 och är förvaltningsövergripande, den gäller därmed för alla verksamheter. I dataskyddsombudets årshjul ligger även utskick med påminnelse och instruktion för uppdatering av registerförteckningen. Utskicket går ut till alla chefer i förvaltningen två gånger per år. Det är dock angeläget att förstå från dataskyddshåll hur pass behjälpligt verksamheterna uppfattar det aktuella stödet, varför detta med fördel skulle kunna undersökas under nästa år genom exempelvis en enkel enkät till dataskyddssamordnare och chefer.

3.1.4 DSO anger hur allvarliga bristerna är på en skala

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

Bristerna som behöver åtgärdas utgörs därmed i huvudsak av tre delar: kvalitén i delar av de befintliga registreringarna behöver höjas med hjälp av stärkt kompetens, i andra fall behöver innehållet kompletteras, samt att registreringar behöver tillkomma från de verksamheter som fortfarande saknas.

3.1.5 DSO ger råd och rekommendationer till PUA

För att höja kvalitén på registreringarna rekommenderas att prioritera kunskapshöjande insatser för dataskyddssamordnare och chefer med fokus på grundläggande begrepp och principer. Det rekommenderas därutöver att fortsätta möjliggöra för dataskyddssamordnare och chefer att kontinuerligt uppdatera och kvalitetssäkra registreringar så att det blir så fullständiga som möjligt.

Det kan i övrigt konstateras att många registreringar saknar angiven risknivå. Arbetet kring att riskbedöma de olika registreringarna bör påbörjas där så inte skett för att den riskkartläggning som ligger till grund för vilka personuppgiftsbehandlingar/processer som behöver konsekvensbedömas ska kunna genomföras av verksamheterna.

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?	Ja
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Ja
Är dokumenten uppdaterade?	Ja
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja

3.2.2 Syfte

Genom styrdokument kommunicerar PUA till medarbetare i sin verksamhet vad som gäller och vad som förväntas av medarbetarna när de hanterar personuppgifter.

Baserat på stadens centrala styrdokument och dataskyddsförordningens krav behöver verksamheten normalt sett ha nedanstående innehåll på plats och antaget lokalt i sin verksamhet i form av styrdokument och rutinbeskrivningar. Som en årligt återkommande aktivitet ska DSO kontrollera om en lämplig uppsättning av grundläggande styrdokument finns upprättade och beslutade. En lämplig tumregel är att tänka att ”det som inte är skrivet finns inte” och att avsaknad av dokumentation därmed är en brist som behöver åtgärdas (även för det fall att det skulle finnas informella/odokumenterade arbetssätt som upplevs fungera väl).

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 dataskyddsarbetet är att viktiga arbetssätt och rutiner ska vara dokumenterade. Detta följer bland annat av kravet på att PUA måste kunna visa att principer för behandling av personuppgifter efterlevs (artikel 5).

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?

Ja, lämplig styrande dokumentation finns på plats och utgörs idag av handbok, rutin för personuppgiftsincidenter, rutin för inventering och registrering av personuppgiftsbehandlingar och rutin för hanteringen av de registrerades rättigheter. Förutom dessa finns även den stadsgemensamma styrningen där bland annat riktlinjer för informationssäkerhet utgör en viktig del. Det finns dock alltid anledning att lyssna in och observera var behov kan finnas av att skapa nya och verksamhetsspecifika rutiner.

För kännedom är ett arbete pågående med att ta fram stödmaterial för verksamheterna i sitt respektive framtagande av information till registrerade (artikel 13), detta utifrån resultatet av den genomförda kartläggningen av informationskravet.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

Ja, existerande dokument är nyligen framtagna och bedöms hålla en lämplig kvalitet.

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

3.2.5 DSO ger råd och rekommendationer till PUA

För att rutinerna ska få önskad effekt behöver de spridas och användas, det rekommenderas därför att dataskydd blir en punkt i verksamheternas APT-årshjul om det ännu inte är det, där rutinerna kan vara ett bra verktyg att utgå ifrån.

PUA rekommenderas även att fortsätta identifiera eventuella behov av ytterligare förvaltningsgemensamma samt verksamhetsspecifika rutiner.

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?	Klassning av fyra system har påbörjats och i dessa återfinns flertalet personuppgiftsbehandlingar. Enskilda personuppgiftsbehandlingar har inte klassats under året.
Är klassade personuppgiftsbehandlingar aktuella?	Kan ej bedömas då den årliga kontroll av aktualitet som enligt stadens riktlinjer för informationssäkerhet ska ske inte har skett.

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 och därmed leva upp till kraven i dataskyddsförordningen. 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.

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

3.3.3 Resultat

I början av året påbörjades klassning av Tempus (system för när- och frånvarorapportering för förskolan) och förvaltningen har i början av året deltagit i ett antal normerande klassningar inom ramen för projektet e-hälsa. Skarpnäck har i samarbete med Farsta stadsdelsförvaltning påbörjat lokala klassningar för två av systemen inom e-hälsa utifrån de normerande resultaten.

Avsaknaden av fler informationsklassningar utgör fortsatt en omfattande brist i stadsdelens dataskydds-och informationssäkerhetsarbete. Informationsklassningarna är viktiga underlag som ligger till grund för de åtgärder som vidtas för att minska och förebygga risker i behandlingen av personuppgifter.

Bristerna bedömdes i 2023 års rapport som allvarliga och har avhjälpts till viss del av att förvaltningen nu har aktiva processer igång för informationsklassningar och att kompetensen i frågorna stärkts under året.

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

Bristerna bedöms vara omfattande och kräva omgående åtgärder från PUA i form av ökad prioritering av informationsklassningar. Informationsklassningar renderar i åtgärder som skyddar information och personuppgifter, men agerar också underlag för exempelvis personuppgiftsbiträdesavtal och möjligheter för verksamheter att nyttja välbehövliga system och tjänster.

3.3.5 DSO ger råd och rekommendationer till PUA

Klassningsarbetet behöver fortsatt prioriteras och stärkas. Vid behov bör det övervägas att ta in hjälp utifrån i form av samarbeten med andra förvaltningar eller av extern konsult.

För att klassningsarbetet sedan ska ge goda resultat när det kommer till skyddet av personuppgifter måste det organisatoriska arbetet i sin tur fungera väl – rekommendationerna och handlingsplanerna som tas fram i klassningsarbetet behöver omhändertas på ett effektivt sätt. Det organisatoriska arbetet kring informationssäkerhet är en viktigt för att vi bland annat ska kunna leva upp till dataskyddsförordningens krav på ansvarsskyldighet, det vill säga vår förmåga att visa hur vi följer de grundläggande principerna såsom att värna människors integritet.

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 en organisation att identifiera och minimera integritetsriskerna för personuppgifter som behandlas. 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 vidtas förebyggande åtgärder.

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), vilket alltså syftar på risken för personers integritet. Dataskyddsförordningens krav på konsekvensbedömning gäller oavsett om behandlingen redan existerade eller inte när dataskyddsförordningen trädde ikraft.

3.4.3 Resultat

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

Nej, förvaltningen har inte identifierat behandlingar som det borde göras konsekvensbedömningar av.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Nej, potentiella högriskbehandlingar har med få undantag inte identifierats och konsekvensbedömts.

Är de genomförda konsekvensbedömningarna aktuella?

En konsekvensbedömning är genomförd under 2024 och bedöms vara aktuell. Ytterligare tre konsekvensbedömningar har påbörjats och förväntas bli klara 2025.

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

Med få undantag saknar förvaltningen fortsatt konsekvensbedömningar för behandlingar som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Det har heller inte kommunicerats till dataskyddsombudet att sådana åtgärder planeras från verksamheterna. Mot bakgrund av detta ges inget utrymme att göra annan bedömning än att det finns allvarliga brister som omgående kräver insatser av ledning och övriga verksamheten på detta område.

3.4.5 DSO ger råd och rekommendationer till PUA

För att komma till bukt med bristen kan verksamheterna med fördel utgå från registerförteckningen, riskbedöma sina personuppgiftsbehandlingar och därefter genomföra tröskelanalyser som i sin tur kommer att svara på vilka behandlingar som kan behöva konsekvensbedömning. IMY och Europeiska datasskyddsstyrelsen (EDPB, European Data Protection Board) har framtagna riktlinjer som talar om när en konsekvensbedömning behöver genomföras, och staden har ett gemensamt och väl utformat metodstöd och mall för själva utförandet.

Konsekvensbedömningar kan även med fördel ske inom ramen för informationsklassningar när det bedöms att en konsekvensbedömning behöver genomföras. Dock ställer inte dataskyddsförordningen krav på informationsklassningar såsom den gör på konsekvensbedömningar (artikel 35). Det är därför inte en framkomlig väg att hänskjuta genomförandet av konsekvensbedömningar till något som tillhör informationsklassning.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	6
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	6

3.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen (artikel 12–22) ett antal rättigheter som på olika sätt ska garantera att den registrerade personen har insyn i hur dennes personuppgifter hanteras samt har en viss kontroll över personuppgiftsbehandlingen. Det är ett krav enligt dataskyddsförordningen att PUA tillgodoser rättigheterna i fråga.

Rättigheterna medför en rätt att ställa krav på att verksamheten vidtar vissa åtgärder, som exempelvis att lämna ut ett så kallat registerutdrag eller att rätta vissa uppgifter. Verksamheten har enligt dataskyddsförordningen artikel 12.3 en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran.

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

klarar av att leva upp till regelverkets krav på att hantera begäran inom föreskriven tidsfrist.

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

Inkomna begäran under året har hanterats inom den angivna tidsfristen och ur det hänseendet finns inga brister av nämnvärd betydelse.

Dock bör det i bedömningen av hanteringen av individens rättigheter vägas in ytterligare aspekter än bara tidsfristen. Dataskyddsförordningen ställer specifika krav i artiklarna 12-22 på hur den personuppgiftsansvariga ska hantera förfrågan och vad svaren bör innehålla. Exempelvis bör svaren på förfrågningarna ges på ett sammanhållet sätt, vara förståeligt och innehålla all behövlig information för att den registrerade ska kunna tillgodogöra sig sina rättigheter. Det har under året tagits fram en rutin med tillhörande bilagor som ska stötta verksamheterna i denna hantering. Denna rutin behöver spridas och tillämpas.

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

Att brister identifierats som bör åtgärdas är alltså inte relaterat till tidsaspekten i hanteringen av förfrågningarna, utan det hittills ojämna och ibland ofullständiga innehållet i själva svaret från personuppgiftsansvarig där det förekommit att det saknats hänvisning till hur den registrerade kan klaga till IMY.

3.5.5 DSO ger råd och rekommendationer till PUA

Det finns idag en framtagen förvaltningsgemensam rutin för hanteringen av registrerades rättigheter publicerad på intranätet.

Denna rutin behöver spridas och tillämpas för att hanteringen ska nå en högre kvalitet när det kommer till innehåll och samordning.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	I de flesta fall uppmärksammas incidenterna av verksamheterna. I andra fall har till exempel felaktiga mottagare av e-post kontaktat verksamheterna
Hur många personuppgiftsincidenter har dokumenterats?	32
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	22 anmälda till Integritetsskyddsmyndigheten, 10 informerat berörda personer
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	18

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.”

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 Integritetsskyddsmyndigheten (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. Alla personuppgiftsincidenter dokumenteras, det vill säga även i de fall då incidenten inte ska rapporteras till IMY där omständigheterna kring personuppgiftsincidenten, dess effekter och vilka korrigerande åtgärder som vidtagits ska framgå. 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?

I ungefär två tredjedelar av fallen har verksamheterna rapporterat personuppgiftsincidenterna i tid. Detta är en förbättring från föregående år då denna siffra utgjordes av en knapp majoritet. Ungefär 69 % av incidenterna har rapporterats till IMY, och i ungefär 31 % av fallen har de registrerade informerats om händelsen.

För kännedom har det under året tagits fram en informationsfilm om personuppgiftsincidenter som bland annat ska kunna visas på verksamheternas APT men också publiceras så att den finns tillgänglig. Informationsfilmen är tänkt att utgöra ett komplement till den rutin som finns publiceras på intranätet.

I denna rapport finns även en särskild granskning av efterlevnaden av förvaltningens nya rutin kring hanteringen av personuppgiftsincidenter, se avsnitt 4.3.

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

Bristerna på detta område bedöms behöva åtgärder eftersom vi fortsatt ser att en relativt hög andel av incidenterna inte rapporterats i tid, något som enligt rapportörerna ofta orsakats av okunskap.

3.6.5 DSO ger råd och rekommendationer till PUA

PUA rekommenderas att återkommande påminna verksamheterna om den rutin som finns skapad för hanteringen av personuppgiftsincidenter. IA är inte optimalt utformat för rapporteringen av personuppgiftsincidenter eftersom det ställs frågor i själva gränssnittet som gör att rapportören leds att tro att denne svarat tillräckligt genom att besvara dessa frågor. Så är dock inte fallet och därför är det aktiva stödet från DSO också viktigt för att höja kvalitén på rapporteringen.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar utifrån 2023 års prioritering:

- Efterlevnaden av den nya rutinen för hantering av personuppgiftsincidenter
- Informationskravet
- Stickprov i eDok – Lex Sarah-ärenden
- Granskning i IA avseende ej inrapporterade personuppgiftsincidenter
- Genomförande av den obligatoriska grundutbildningen i dataskydd
- Övriga granskningar enligt årshjul, sammanfattning

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

Efterlevnaden av den nya rutinen för hanteringen av personuppgiftsincidenter

Under slutet av 2023 publicerades en ny rutin för hanteringen av personuppgiftsincidenter för stadsdelsförvaltningen. Den nya rutinen innebar bland annat att rapporteringen vid inträffad personuppgiftsincident sker i incidentrapporteringssystemet och att tydligare ansvar läggs på enhetschef för att utredningen av händelsen ska ske korrekt. Dataskyddsombudet ska alltid informeras och kan rådfrågas.

I rutinen har tydliggjorts vilken information som rapportör och ansvarig enhetschef måste se till att den finns. Det handlar bland annat om hur många registrerade som drabbats, hur många personuppgiftsposter det handlar om och tidpunkterna för incident och upptäckt. Dokumentationskravet framgår i dataskyddsförordningen artikel 33.

En annan del i den nya rutinen är att beslut ska fattas i de fall bedömningen görs att incidenten inte ska anmälas till Integritetsskyddsmyndigheten, och/eller att den/de registrerade inte ska informeras om incidenten. Beslutstypen framgår av stadsdelsförvaltningarnas hanteringsanvisningar och ska diarieföras i eDok. Dessa beslut med avdelningschef som lägsta delegat fattas i mycket liten omfattning idag och stora förbättringar på området behöver ske. Korrekt och fullständig dokumentation är viktig för att förvaltningen ska leva upp till den grundläggande principen om ansvarsskyldighet.

Av femton granskade incidenter är det endast tre som lever upp till dokumentationskravet. Resultatet visar därmed på stora brister och förvaltningen kan i dagsläget inte sägas leva upp till kraven i dataskyddsförordningen. Bristerna bedöms därför vara omfattande och kräva omgående åtgärder.

	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

DSO ger råd och rekommendationer till PUA
PUA rekommenderas att återkommande påminna verksamheterna om att använda sig av rutinen för hantering av personuppgiftsincidenter. Särskilt viktigt är det vid rapportering i IA eftersom gränssnittet inte är anpassat efter de krav som ställs i dataskyddsförordningen. Vidare bör även vikt läggas på dokumentationskravet på beslut när personuppgiftsincidenter inte anmäls till Integritetsskyddsmyndigheten.

Stickprov i eDok, granskning av Lex Sarah-ärenden utifrån principen om uppgiftsminimering samt integritet och konfidentialitet

Dataskyddsförordnigen har sju grundläggande principer varav uppgiftsminimering är en, och integritet och konfidentialitet är en annan. Stickprov har genomförts av Lex Sarah-ärenden som inkommit eller upprättats under året. Sex stycken registreringar har granskats. Valet av ärendeslaget utgår ifrån ett riskbaserat arbetssätt, Lex Sarah-utredningar berör personer som på olika sätt befinner sig i en utsatt ställning och händelserna i sig kan vara av känslig natur. Det är därför viktigt utifrån ovan nämnda dataskyddsliga principer att dokumentationen sker på ett så objektivt och icke-utlämnande sätt som möjligt samt att tillgången till informationen skyddas med hjälp av behörighetsbegränsning. Denna granskning har avgränsats till att titta på fyra frågeställningar med utgångspunkt i principerna: 1. Hur många har tillgång till ärendet i verksamhetssystemet? 2. Jobbar dessa personer kvar i förvaltningen? 3. Har personuppgifter registrerats i registreringsvyn i eDok? 4. Innehåller rapporterna identifierande personuppgifter?

Granskningen visade vidare att det endast i ett fall förekom namn på person som varit föremål för rapporten. Det kan konstateras att det i detta fall framkom i en mall framtagen av staden där de

identifierande personuppgifterna efterfrågades av staden. I övriga fall har inga identifierande personuppgifter förekommit. Vad gäller behörighetsbegränsningen var den också aktuell och korrekt i alla kontrollerade ärenden. I inget fall hade personuppgifter registrerats i eDoks registreringsvy.

I förvaltningens rutiner för Lex Sarah-hantering framgår att inga identifierande personuppgifter ska förekomma i rapporteringen.

	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

DSO ger råd och rekommendationer till PUA
Den brist som identifierats härrör till en otydlighet kring vilken information som efterfrågas i de olika mallarna. Dessa kan dock inte anpassas av förvaltningen för att överensstämma med riktlinjerna för hanteringen, och därmed inte efterfråga till exempel namn och personnummer på drabbade personer. Enligt rutin ska verksamheterna i den mån det går undvika att dokumentera personuppgifter som gör det möjligt att spåra den enskilde. Detta är något cheferna bör fortsätta att påminna om.

Informationskravet

Enligt dataskyddsförordningen ska det vara klart och tydligt för de registrerade hur den personuppgiftsansvariga behandlar deras personuppgifter. Förvaltningen behöver alltså informera om när personuppgifter samlas in, varför de samlas in och hur de sedan används. De registrerade ska också veta vad de har för rättigheter, till exempel hur de kan få felaktiga uppgifter rättade och hur de kan få personuppgifter raderade. De registrerade måste därför få information om allt detta, och det ska ske senast vid insamlandet av personuppgifter. Informationen ska vara lätt att hitta och den ska vara formulerad på ett sätt som är enkelt och begripligt.

I början av året gjordes en översikt för att se huruvida verksamheterna hade rutiner för att leva upp till informationskravet. Kartläggningen visade att bara 18 % av de svarande enheterna hade rutiner för att informera personer om hur de behandlar deras personuppgifter. Till viss del uppfylls kravet av den generella information som går att tillgå på stadens webbsida om hur staden behandlar personuppgifter och som många kollegor hänvisar till i sin mejlsignatur. Denna information är dock generell och inte att anse som tillräcklig. Mot bakgrund av att en stor majoritet idag saknar rutiner för detta bedöms bristerna på detta område vara omfattande och kräva omgående åtgärder.

	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

DSO ger råd och rekommendationer till PUA

Ett framtagande av stödmaterial till verksamheterna är pågående. Detta material ska stödja verksamheterna i det egna framtagandet av informationen till registrerade.

I den mån verksamheter ser fördelar med att samordna informationen med varandra kan detta vara ett bra alternativ. Det rekommenderas särskilt att kontakta sina motsvarigheter i andra stadsdelar för att ta del av deras information och erfarenheter.

Granskning i IA avseende ej inrapporterade personuppgiftsincidenter

Den 4 oktober granskades samtliga registrerade incidenter i IA under 2024 för att kontrollera om det rapporterats in incidenter som också skulle ha rapporterats som personuppgiftsincidenter. Tre incidenter gällande borttappade enheter (dator/telefon) lokaliserades och ansvariga chefer fick återkoppling om att händelserna även är att betrakta som personuppgiftsincidenter.

	Allvarliga brister iedentifierade 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

DSO ger råd och rekommendationer till PUA
Det rekommenderas att IT-samordnare/strateg bör ha information till medarbetare som anmäler borttappade enheter om att händelserna även är att betrakta som personuppgiftsincidenter.

Genomförande av den obligatoriska grundutbildningen i dataskydd
För att förvaltningen ska kunna leva upp till kraven i dataskyddsförordningen behöver grundläggande kunskaper om dataskydd upprätthållas bland medarbetare och chefer. Staden har beslutat att alla medarbetare årligen ska genomföra grundutbildning i dataskydd.

Av totalt 843 tillsvidareanställda medarbetare har 168 genomfört utbildningen.

Resultaten visar att ungefär 20 % hade statusen genomfört vid tidpunkten för rapporten. Det tillgängliga underlaget talar inte om hur långt de medarbetare kommit som påbörjat utbildningen men ej slutfört. Resterande hade ej genomfört utbildningen.

Tidigare årsrapport är baserad på antalet timanställda som antingen har genomfört, påbörjat eller inte påbörjat utbildningen, men omfattade inte det totala antalet timanställda på förvaltningen. Dessutom har det sedan december 2023 tillkommit sex gruppbostäder LSS i egen regi. Av dessa anledningar är den procentuella andelen som har genomfört utbildningen lägre än tidigare år.

Eftersom underlaget inte visar vilka som har påbörjat utbildningen går det inte heller att dra några definitiva slutsatser om antalet vad gäller genomförande eftersom det lika gärna kan vara ett knapptryck som saknas så väl som större delen av utbildningen.

Eftersom utbildningen är obligatorisk är den eftersträvansvärda siffran högre än 80 % för genomförande, och att siffran genomfört vid tillfället enbart var 20 % indikerar att uppföljningen från cheferna har omfattande brister i behov av omgående åtgärder.

Övriga granskningar enligt årshjul, sammanfattning

I dataskyddsombudets årshjul ligger ett flertal återkommande granskningar för att följa upp hur förvaltningen följer dataskyddslagstiftningen. Bland annat så kontrolleras förekomsten av PUB-avtal. Resultatet av kontrollen i år visade att förvaltningen har ett antal tecknade PUB-avtal som bedöms vara aktuella, och det uppmärksammades även fall där PUB-avtal med leverantör saknades. I dessa fall har ansvarig chef kontaktats för att åtgärda detta. Stadsintern instruktion mellan nämnden och stadsledningskontoret har under året tecknats för tillhandahållandet av tjänsten eVald, och framtagande av stadsintern instruktion mellan nämnden och Serviceförvaltningen är pågående. Det finns även fall som uppmärksammats under genomgången där personuppgiftsansvarig behöver teckna PUB-avtal men där detta bör föregås av en informationsklassning, bland annat för att rätt krav ska ställas på leverantörens säkerhetsåtgärder.

Ett urval av förvaltningens sociala medier-konton har granskats för att se att om det finns information om hur personuppgifter hanteras i kontot (t.ex. informationstext eller länk till stadens integritetspolicy) samt om ansvarig verksamhet kan visa att det finns dokumenterade samtycken för fotografier. I de granskade exemplen fanns behov av komplettering vad gäller information om personuppgiftsbehandling och återkoppling gavs till ansvarig person, och förtydliganden gjordes gällande hur samtycken ska behandlas.

DSO ger råd och rekommendationer till PUA
Gällande personuppgiftsbiträdesavtal så rekommenderas att vid samtliga avtalsuppföljningar där det finns ett personuppgiftsavtal följa upp om hanteringen av personuppgifter förändrats i någon mån. Att vid nya upphandlingar kontakta dataskyddsombudet vid behov för att rådgöra om personuppgiftsbiträdesavtal behöver tecknas. Det rekommenderas även att förvaltningen i de fall det avser system eller andra typer av IT-tjänster genomför informationsklassningar för att innehållet i avtalen ska bli korrekt.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- *Bristande kunskaper i dataskyddsfrågor*
- *Hanteringen av känsliga personuppgifter som kan innebära hög risk för registrerades fri- och rättigheter*

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

Bristande kunskaper i dataskyddsfrågor

I tidigare års GDPR-rapporter har bristande kunskaper i dataskyddsfrågor lyfts fram som en av de mest centrala riskerna när det kommer till personuppgiftshanteringen i förvaltningen. Detta bedöms även kvarstå under 2024.

Bristande kunskaper om dataskyddsförordningen och de krav förordningen ställer på personuppgiftshantering innebär en risk av flera skäl. Utan kunskap blir det svårt att upptäcka säkerhetsrisker kring personuppgiftshantering. Det är också svårt att då uppfylla de grundläggande principerna såsom information till registrerade om hur deras personuppgifter behandlas, principen om lagringsminimering eller principen om ändamålsminimering, det vill säga att personuppgifter enbart får användas för de syften som de först samlades in för. Bristande kunskaper kan också öka risken för att personuppgiftsincidenter sker, samt att förvaltningen inte på ett korrekt sätt arbetar förebyggande mot risker.

	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

Bristerna på området bedöms inte vara omfattande och i behov av omgående åtgärder. Skillnader mellan enheter finns men gemensamt är att dataskyddsfrågorna fortsatt behöver integreras på ett sätt som gör det lätt att göra rätt och att rätt stöd finns tillgänglig när så behövs. Idag har ett flertal rutiner tagits fram som kan fungera som stöd för verksamheterna.

Hanteringen av känsliga personuppgifter som kan innebära hög risk för registrerades fri- och rättigheter

Även detta år visar resultaten av de obligatoriska rapporteringsområdena tekniska och organisatoriska skyddsåtgärder samt konsekvensbedömningar på omfattande och allvarliga brister. Förvaltningen har fortsatt inte på ett systematiskt och dokumenterat sätt identifierat och minimerat de risker som behandling av integritetskänsliga personuppgifter kan innebära. Hanteringen av känsliga personuppgifter som kan innebära hög risk för registrerades fri- och rättigheter bedöms därför vara ett kvarvarande riskområde.

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

Eftersom förvaltningen idag på bred front saknar riskanalyser, konsekvensbedömningar för högriskbehandlingar och till viss del saknar organisatoriska åtgärder när det kommer till

informationssäkerhet kan det inte sägas att förvaltningen lever upp till kraven som dataskyddsförordningen ställer på hanteringen av känsliga personuppgifter som kan innebära hög risk för registrerades fri- och rättigheter.

5.4 DSO ger råd och rekommendationer till PUA

Utifrån den kvarstående risken kring kunskap om dataskydd rekommenderas det att genomföra riktade utbildningsinsatser med särskilt fokus på chefer och dataskyddssamordnare för att stärka kompetens och initiativförmåga.
När det kommer till risken kopplat till hanteringen av känsliga personuppgifter kan den avhjälpas genom att förvaltningen, utifrån ett riskbaserat arbetssätt, klassar och konsekvensbedömer system och behandlingar där känsliga personuppgifter hanteras i stora mängder så att risker kan förebyggas på det sätt som dataskyddsförordningen kräver.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Årsrapporten innehåller ett antal obligatoriska rapporteringsområden som återfinns i avsnitt 3. Det har påvisats stora brister på områdena tekniska och organisatoriska skyddsåtgärder samt konsekvensbedömningar, och dessa kommer därmed fortsatt vara centrala i dataskyddsombudets granskande arbete under nästkommande år. Utöver dessa övergripande områden, har följande granskningsområden inom förvaltningens verksamheter bedöms vara relevanta:

- *Registerförteckningen*
- *Personuppgiftsincidenter, kvalitativ granskning med fokus på orsak och åtgärd*

6.2 Syfte

Det granskande arbetet är som tidigare nämnt 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

Registerförteckningen
Som tidigare konstaterat består i dagsläget bristerna i registerförteckningen i huvudsak av tre delar; kvalitén i delar av de befintliga registreringarna behöver höjas med hjälp av stärkt kompetens, i andra fall behöver innehållet kompletteras, samt att registreringar behöver tillkomma från de verksamheter som fortfarande saknas. Verksamheterna har fått information om den granskning som skett enligt årshjulet men det finns fortfarande behov av att undersöka bristerna ytterligare i en mer djupgående granskning för att registerförteckningen ska bli fullständig.

6.3.1 DSO ger råd och rekommendationer till PUA

För att höja kvalitén på registreringarna rekommenderas att prioritera kunskapshöjande insatser för dataskyddssamordnare och chefer med fokus på grundläggande begrepp och principer. Det rekommenderas därutöver att fortsätta möjliggöra för dataskyddssamordnare och chefer att kontinuerligt uppdatera och kvalitetssäkra registreringar så att det blir så fullständiga som möjligt.

Det kan i övrigt konstateras att många registreringar saknar angiven risknivå. Arbetet kring att riskbedöma de olika registreringarna bör påbörjas där så inte skett för att den riskkartläggning som ligger till grund för vilka personuppgiftsbehandlingar/processer som behöver konsekvensbedömas ska kunna genomföras av verksamheterna.

Personuppgiftsincidenter, kvalitativ granskning
Särskild uppföljning planeras av personuppgiftsincidenter med fokus på angivna åtgärder och uppföljning. För att få en bild av orsaker till personuppgiftsincidenter och hur de hanteras samt följs upp är det viktigt att förvaltningen fortsätter att granska för att jobba med

förbättringar. Ett antal stickprov planeras genomföras där verksamheterna får besvara hur åtgärderna på personuppgiftsincidenter som angivits i IA har efterlevts. Inriktningen på frågorna kommer avse hur rutinerna på verksamheterna ser ut, vilka åtgärder som har vidtagits efter personuppgiftsincidenter samt huruvida dessa finns dokumenterade på något vis. Uppföljning av åtgärderna kommer också att undersökas. Granskningen kommer ske löpande samt under slutet av år 2025 när sammanställningen av årets personuppgiftsincidenter gjorts.

7 Övrigt att rapportera

Styrningen i dataskyddsarbetet

Som konstaterat i 2023 års rapport är målsättningen att dataskyddsarbetet ska vara en integrerad del i verksamheternas arbete. För att dataskyddsombudet ska kunna genomföra både sitt granskande och utbildande arbete på ett effektivt sätt behöver det finnas uppföljningsmekanismer, där årshjulet är ett sådant verktyg. Utöver det så behöver även chefer ha goda förutsättningar att integrera dataskyddet i verksamheterna, och för att detta ska förverkligas behöver de insatser som ska genomföras vara begripliga och tillgängliga, det vill säga det ska vara tydligt varför och hur och när vissa kontroller, analyser, riskbedömningar eller andra åtgärder ska ske. För att förvaltningen i högre utsträckning ska leva upp till de krav som ställs i dataskyddsförordningen behöver frågorna hanteras systematiskt och konsekvent. Erfarenheten från året är att dataskyddsarbetet fortsatt sker punktvis och ofta på uppmaning av ombudet snarare än strategiskt på uppmaning av ledningen. För att komma vidare skulle det omvända förhållandet behöva råda.

Personuppgifter i e-post

Ett stadsövergripande och omfattande problem för dataskyddet är att det hittills inte har varit möjligt att skicka e-post innehållande personuppgifter på ett helt säkert sätt. Stadens interna mejl är skyddad vid överföringen genom kryptering, men inte när den ligger i någon av Outlookkorgarna. För de medarbetare som har Fujitsuleveransen finns inget sådant skydd. Staden har möjliggjort användande av Säkra meddelanden, men förvaltningen har valt att inte införa användningen av tjänsten innan en lokal informationsklassning och konsekvensbedömning har genomförts. Detta behöver därför prioriteras högt under 2025.

Åtgärdsplan för områden med brister

Eftersom ett flertal av årets granskningsområden har visat sig ha brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheter så har förvaltningen upprättat en åtgärdsplan. I åtgärdsplanen identifieras de områden med omfattande förbättringsområden tillsammans med konkreta förslag på aktiviteter och ansvarsområden som kan åtgärda bristerna. Åtgärdsplanen kommer tillsammans med årshjulet ligga som grund för det nästkommande årets dataskyddsarbete och följas upp under året.