Stockholms stad

Bilaga 03

GDPR Årsrapport

År 2024

Södermalms stadsdelsnämnd

GDPR årsrapport
Januari 2025

Dnr: SÖD 2024/1142
Utgivningsdatum: 2025-02-20
Kontaktperson: Anna Remmets

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 jag följande årsrapport.

2023 års granskning omfattade de sex obligatoriska rapporteringsområdena. 2024 har utöver dessa två ytterligare områden, uppgifts- och lagringsminimering samt personuppgiftsbiträdesavtal, granskats. Årets granskning visar att riskerna har minskat på ett flertal områden i jämförelse med 2023.

0 st. (2023: 0 st.)	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
0 st (2023: 2 st.)	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
5 st (2023: 4 st.)	Brister identifierade som bör åtgärdas men som inte bedöms vara brådskande, omfattande eller allvarliga
1 st (2023: 0 st.	Inga brister av nämnvärd betydelse identifierade

Nämnden bedöms i nuläget inte ha några ”orange” nivåer och har nått ner till ”grönt” på ett område. Att merparten av riskerna fortfarande bedöms som ”gula” beror till största del på att redan påbörjade arbeten behöver fortsätta och utvecklas. De flesta av dessa bygger på att förvaltningen fortsätter att implementera ändamålsenlig rutin och organisation för informationssäkerhetsarbete.

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 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?	478
Har nödvändiga uppdateringar gjorts?	Delvis
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

För att något ska gå att skydda måste det först vara synligt för verksamheten. Det följer därför i klartext av dataskyddsförordningen (artikel 30) 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.

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.

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

Antalet registrerade behandlingar fortsätter att öka. Ökningen har planat ut efter den insats som gjordes med hjälp av konsult, men det var förväntat.

DSO kontrollerar om nödvändiga uppdateringar gjorts

I december 2024 hade dataskyddsredogörare på fyra av förvaltningens sju avdelningar rapporterat att de fått bekräftelse från ansvariga chefer på att förteckningen är uppdaterad.

DSO:s bedömning är att ytterligare uppdateringar behöver göras på samtliga avdelningar.

DSO bedömer hur fullständig registerförteckningen är

Stora förbättringar har skett men DSO:s bedömning (utifrån bland annat stadens hanteringsanvisningar) är att alla verksamhetsprocesser där personuppgifter behandlas ännu inte är förtecknade.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Under 2024 har förvaltningen fortsatt att utveckla rutinerna för registerföring. Det intensifierade arbetet med informationsklassningar skapar bättre förutsättningar för att

förteckna personuppgiftsbehandlingar då det finns med som ett krav i klassningsverktyget Klassa.

Förvaltningen har också infört en halvårsvis kontroll där dataskyddsredogörarna skickar standardiserade uppdateringsfrågor till ansvariga chefer. Responsen på dessa har dock varierat (se ovan samt delgranskningsrapport Personuppgiftsförteckningar december 2024, dnr SÖD 2024/552).

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 som inte bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.1.5 DSO ger råd och rekommendationer till PUA

Det är viktigt att det hos både chefer och lokala objektledare finns en förståelse för personuppgiftsförteckningens funktion och syfte, och att det finns förståelse för att den/de som ansvarar för och äger verksamhetsprocesserna också ansvarar för att förteckningen är uppdaterad avseende den egna avdelningen/enheten och för att dataskyddsredogörarna förses med korrekta underlag. DSO kan med fördel bjudas in till APT, ledningsgrupper och liknande för att informera ytterligare.

Det är också viktigt att dataskyddsredogörarna får tid och förutsättningar för att utföra sitt uppdrag.

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?	Delvis
Är dokumenten uppdaterade?	Ja
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja

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?

Lämplig styrande dokumentation finns på plats i form av centrala och lokala styrdokument och rutiner.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

DSO:s bedömning är att både de centrala och lokala dokumenten håller lämplig kvalitet och är uppdaterade. Utmaningen ligger snarare i att vissa dokument, i synnerhet den lokala anvisningen för informationssäkerhet, skulle behöva bli känd i högre grad.

Se även delgranskningen om styrdokument, SÖD 2024/552.

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 som inte bedöms vara brådskande, omfattande eller allvarliga
x	Inga brister av nämnvärd betydelse identifierade

3.2.5 DSO ger råd och rekommendationer till PUA

Under 2024 har Informationssäkerhetssamordnaren (ISAM) och DSO tillsammans sett över vilka dokument inom deras områden som behöver uppdateras, vilka som kan sammanföras, samt behov av nya rutiner och styrdokument. Detta arbete bör fortsätta under 2025.

Enheterna bör även fortsättningsvis rapportera i ILS huruvida dokumenten är kända bland medarbetarna och hur de har gjorts kända.

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?	Det är svårt att ange ett exakt antal eftersom personuppgiftsförteckningen inte bedöms vara helt komplett, men totalt har 44 system klassats och samtliga av dessa bedöms innehålla någon typ av personuppgiftsbehandlingar.
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.

3.3.3 Resultat

Under 2024 har förvaltningen bedrivit ett intensivt arbete med informationsklassningar. I princip alla system och informationsmängder som har klassats innehåller personuppgifter.

Under 2024 har ISAM tillsammans med informationssäkerhetskonsult också utvecklat rutiner för uppföljning av klassningar för att kunna säkerställa att åtgärder i åtgärdsplanerna följs upp och att informationen därmed får rätt skydd.

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 som inte bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.3.5 DSO ger råd och rekommendationer till PUA

Arbetet med informationsklassningar bör fortsätta, och det är också viktigt att de åtgärder som beslutats implementeras och följs upp.

För att detta ska kunna ske bör förvaltningen fortsatt arbeta med att etablera strukturen med lokala objektledare samt med informationsinsatser till lokala objektledare, processägare och chefer så att förståelsen ökar för när i processen informationsklassningar behöver ske, hur ansvaret är fördelat och hur uppföljningar av beslutade åtgärder ska genomföras.

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 en organisation att identifiera och minimera integritetsriskerna för personuppgifter som behandlas i projekt eller linjeverksamhet. 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/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).

3.4.3 Resultat

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

DSO:s bedömning är att inte alla, men många, av förvaltningens högriskbehandlingar har identifierats. Förmågan att identifiera dessa

hänger ihop med det pågående arbetet med att genomföra informationsklassningar och uppdatera registerförteckningen. Genom detta arbete har förutsättningen för att upptäcka högriskbehandlingar förbättrats.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Nej (se ovan).

Är de genomförda konsekvensbedömningarna aktuella?

Lokala objektledare har vid tidigare granskning av de då aktuella konsekvensbedömningarna bekräftat deras aktualitet eller kompletterat. Under 2024 kommer DSO och ISAM se över hur uppföljning av konsekvensbedömningar och informationsklassningar kan samordnas.

3.4.4 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 som inte bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.4.5 DSO ger råd och rekommendationer till PUA

Förmågan att identifiera personuppgiftsbehandlingar som innebär en hög risk för registrerades integritet hänger samman med det övergripande arbetet med informationsklassningar och uppdatering av personuppgiftsförteckningen. Om dessa arbetssätt fortsätter att utvecklas såsom beskrivits ovan finns därför goda förutsättningar att identifiera behandlingar som kräver konsekvensbedömning.

Liksom i det övriga informationssäkerhetsarbetet behöver det finnas ett tydligt ansvar över de åtgärder som beslutas, eftersom det är genom dessa åtgärder risker kopplat till integritet sänks till en acceptabel nivå.

Förvaltningen behöver även följa utvecklingen av AI-funktioner då dessa kan innebära integritetsrisker som gör att konsekvensbedömning blir nödvändig.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	7 st. under 2024
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	7 st.

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 förordningen att den verksamhet som enligt förordningen är att se som personuppgiftsansvarig – dvs. i stadens fall nämnder och bolag – 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. (Radering, den så kallade ”rätten att bli glömd”, är sällan aktuell i någon större mån eftersom stadens verksamheter lyder under krav på bevarande till följd av offentlighetsprincipen.) Verksamheten har enligt dataskyddsförordningen artikel 12.3 en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran. (Notera dock att det finns undantagssituationer angivna i artikel 12.3, där fristen kan förlängas till mer än en månad.)

Dataskyddombudet har en roll i att granska efterlevnaden, identifiera brister samt ge råd och stöd hur processer och rutiner för att tillgodose rättigheterna bör utformas.

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

DSO:s bedömning är att kunskapen på förvaltningen om hur registrerades rättigheter ska hanteras har ökat. En lokal rutin finns. Det finns dock osäkerhetsmoment kring leverantörernas förutsättningar att göra informationsuttag i den omfattning och inom den tidsfrist som artikel 15 GDPR anger.

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 som inte bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.5.5 DSO ger råd och rekommendationer till PUA

ISAM, DSO och arkivarier bör såsom diskuterats inom dessa funktioner samverka både med varandra och med stadsledningskontorets juridiska avdelning för att se hur tekniska förutsättningar och kunskap kring att hantera förfrågningar om allmänna handlingar och rättighetsutövande enligt GDPR.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Rapporteras direkt till DSO enligt rutin eller upptäcks vid DSO:s regelbundna kontroller i IA.
Hur många personuppgiftsincidenter har dokumenterats?	23 st.
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	6 st. har rapporterats till IMY. 10 st. incidenter har meddelats de registrerade.
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	2 st.

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 del av dataskyddsförordningens olika verktyg för att åstadkomma en sund personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering.

Stadens mall för DSO:s årsrapport är avsedd att fokusera på rapporteringen.

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag från rapporteringsskyldigheten gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” (se artikel 33). Detta innebär att de flesta personuppgiftsincidenter ska rapporteras till IMY, inte senare än 72 timmar efter att verksamheten fått vetskap om incidenten. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter och friheter, ska rapportering även ske till de berörda registrerade personerna, utan dröjsmål. Dataskyddsförordningen delar alltså in personuppgiftsincidenter i tre kategorier: ingen rapportering, rapportering till IMY samt rapportering till de berörda personerna.

Bristande förmåga att rapportera personuppgiftsincidenter i tid kan leda till sanktioner från IMY:s sida.

Notera att enligt dataskyddsförordningen artikel 33.5 ska alla personuppgiftsincidenter dokumenteras, det vill säga även i de fall då incidenten inte ska rapporteras till IMY. Bristande dokumentering står i strid med Dataskyddsförordningen och leder även till problem med att ta fram korrekta siffror till årsrapporteringen avseende hur väl verksamheten lever upp till rapporteringsfristerna. Enligt artikel 33.5 är det ett krav att dokumentera omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden och bristande dokumentering är sanktionsgrundande.

3.6.3 Resultat

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

För merparten av de personuppgiftsincidenter som har rapporterats under 2024 har det bedömts som osannolikt att de skulle leda till risker för fysiska personers rättigheter och friheter och det har i de fallen endast upprättats interna incidentrapporter. I de sex fall där bedömningen har gjorts att incidenten behövt rapporteras till IMY har detta dock bara skett i tid i två av fallen. I tre av de resterande

berodde förseningen på att DSO inte fått kännedom om det inträffade (i det fjärde fallet på utredningstid).

Att färre incidenter än 2023 har varit av den allvarlighetsgrad att de behövts rapporteras till IMY är dock positivt (2023 var antalet 16). Det sammanlagda antalet personuppgiftsincidenter ligger kvar på i stort sett samma nivå som föregående år: 27 2023 och 23 2024.

Lokalrutin för incidenthantering finns och en extra informationsinsats gjordes på DSO:s återkommande utbildning hösten 2024.

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 som inte bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.6.5 DSO ger råd och rekommendationer till PUA

Alla medarbetare behöver genom utbildningar och information på APT fortsatt påminnas om rutinen för att rapportera personuppgiftsincidenter och vikten av att göra det i tid.

4 Genomförda granskningar under året

4.1 Sammanfattning

Under 2024 har DSO utöver de ovan beskrivna obligatoriska granskningsområdena genomfört följande granskningar:

- Uppgifts- och lagringsminimering.
- Personuppgiftsbiträdesavtal

4.2 Syfte

Syftet med att granska uppgifts- och lagringsminimering är att två av de mest grundläggande principerna för en laglig personuppgiftsbehandling i enlighet med bestämmelserna i dataskyddsförordningen GDPR är uppgifts- och lagringsminimering. Uppgiftsminimering betyder att inte fler personuppgifter än vad som krävs för det angivna syftet behandlas och lagringsminimering betyder att dessa inte sparas längre än nödvändigt. I Stockholms stad får dock inte heller uppgifter raderas om det inte finns ett tillämpligt gallringsbeslut.

Syftet med att granska personuppgiftsbiträdesavtal är att många nödvändiga krav och åtgärder på säkerhet för personuppgifter regleras i personuppgiftbiträdesavtal med leverantörer. Att sådana tecknas vid behov är därför nödvändigt för en lämplig nivå av dataskydd.

4.3 Genomförda granskningar och deras resultat

Uppgifts- och lagringsminimering

	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 som inte bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

Förvaltningen följer stadens hanteringsanvisningar och har en etablerad arkivorganisation. Granskningen visar dock att det finns oklarheter kring vad som får sparas på samarbetsytor och gruppdiskar och hur dessa lagringsytor ska kontrolleras.

Granskningen visar också att dokumentation av lagringsfrister i personuppgiftsförteckningen har brister vilket kan vara en indikation på bristande kännedom om hur länge uppgifterna i fråga ska sparas.

Se även granskningsrapport Uppgifts- och lagringsminimering, SÖD 2024/552.

Personuppgiftsbiträdesavtal

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

Granskningen indikerade att det finns situationer där Personuppgiftsbiträdesavtal (PUB-avta) antagligen skulle behövas med där sådant inte fanns, men också situationer där det är tveksamt om befintligt PUB-avtal är nödvändigt och korrekt. I synnerhet när det gäller de situationer där nämnden är biträde åt privata utförare behöver PUB-avtal tecknas, även om det också är de personuppgiftsansvariga utförarnas ansvar.

Generellt behöver kunskapen om när man behöver ta ställning till tecknande av PUB-avtal och kontakta förvaltningens DSO för stöttning öka. I vissa fall är biträdessituationen mer komplicerad än den först kan verka, och det finns inte alltid samsyn mellan parterna om hur denna ser ut.
Förutsättningen för att i tid undersöka eventuella biträdessituationer har dock förbättrats i och med det utvecklade arbetssättet för informationsklassning.

Se även granskningsrapport Personuppgiftsbiträdesavtal, SÖD 2024/552.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- Förvaltningen har inte full kontroll över sina personuppgiftsbehandlingar och kan inte visa hur de lever upp till Dataskyddsförordningens krav.
- Åtgärder som har beslutats implementeras inte/följs inte upp.

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

Förvaltningen har inte full kontroll över sina personuppgiftsbehandlingar och kan inte visa hur de lever upp till Dataskyddsförordningens krav.

	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 som inte bedöms vara brådskande, omfattande eller allvarliga

	Inga brister av nämnvärd betydelse identifierade

Detta är fortsatt en risk då personuppgiftsförteckning ännu inte är helt fullständig och uppdaterad. Att risken lyfts trots att betydande förbättringar har gjorts beror på att personuppgiftsförteckningen är förutsättningen för flera delar av efterlevnad till GDPR såsom att kunna identifiera riskfyllda behandlingar, tillgodose registrerades rättigheter och dokumentera hur man lever upp till lagstiftningens krav.

Åtgärder som har beslutats implementeras inte/följs inte upp

	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 som inte bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

Arbetet med att skydda information inklusive personuppgifter har utvecklats betydligt. Arbetet med att implementera och följa upp beslutade åtgärder behöver dock fortsätta och därmed finns det fortfarande en risk att åtgärder inte genomförs och att informationen inte får rätt skydd.

5.4 DSO ger råd och rekommendationer till PUA

Se kapitlen om personuppgiftsförteckningen samt tekniska och organisatoriska åtgärder för DSO:s rekommendationer till PUA.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Inbyggt dataskydd och dataskydd som standard
- Autentisering

6.2 Syfte

Syftet med att granska inbyggt dataskydd och dataskydd som standard är att artikel 25 i dataskyddsförordningen GDPR fastslår att den personuppgiftsansvariga är skyldig att implementera inbyggt dataskydd och dataskydd som standard. Inbyggt dataskydd betyder att dataskydd ska tas i beaktande redan innan en tjänst upphandlas/börjar användas och dataskydd som standard betyder att grundinställningarna ska överensstämma med principerna för dataskydd. Till exempel ska inte uppgifter automatiskt sparas för att sedan vara sökbara i textfält.

Autentisering är en form av inbyggt dataskydd. Då förvaltningen behandlar en stor mängd känsliga uppgifter om personer i beroendeställning och dessutom behöver kunna använda digitala lösningar är autentisering en viktig del av den åtkomstbegränsning som är nödvändig för att kunna hantera denna typ av information på ett säkert sätt.

6.3 Planerade granskningar

Inbyggt dataskydd och dataskydd som standard

Denna granskning kommer primärt att ske genom att DSO gör stickprov i informationsklassningar och i personuppgiftsförteckningen. I dessa kan utläsas vilka tekniska och organisatoriska lösningar som finns för dataskydd och vilka åtgärder som beslutats.

Autentisering

DSO gör stickprover i informationsklassningar och i personuppgiftsförteckningen men kan eventuellt också ställa frågor till relevanta roller inom förvaltningen.