Stockholms stad

Bilaga 03

GDPR Årsrapport

År 2023

Södermalms stadsdelsnämnd

GDPR årsrapport
Januari 2024
Dnr: 2023/1037
Utgivningsdatum: 2024-02-22
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 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:s 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 (DSO) lämnar jag följande årsrapport.

Under 2023 har Södermalms stadsdelsförvaltning intensifierat arbetet med informationssäkerhet inklusive dataskydd. Till exempel har konsulter anlitats för att hjälpa till med personuppgiftsförteckningen och informationsklassningarna. Detta har lett till att antalet registrerade personuppgiftsbehandlingar i Draftit har ökat markant, vilket lett till att bristerna nu är på en gul nivå till skillnad mot orange i årsrapporten för 2022.

Att vissa brister är kvar på en oförändrad nivå eller till och med höjts kan dels bero på att bedömningen är att ytterligare åtgärder krävs för att nå en ”grön nivå” då denna definieras som ”Inga brister av nämnvärd betydelse identifierade”, dels att ny kunskap eller information har lett till en ny bedömning.

Det sistnämnda är fallet med rapporteringsområdena Tekniska och organisatoriska åtgärder och Individens rättigheter. Vad gäller tekniska och organisatoriska åtgärder så är implementeringen av sådana beroende av att informationssäkerhet inklusive dataskydd omhändertas från början i förvaltningens processer. För att detta ska kunna ske behöver dock förvaltningen fortsätta arbetet med att rollbesätta i enlighet med it-styrningsmodellen PM3.

För uppfyllandet av individens rättigheter att bland annat begära information om hur hens personuppgifter behandlas måste det finnas fungerande rutiner för beställning av information från stadens it-leverantörer. Ett aktuellt fall har visat att det behövs en genomlysning av hur detta fungerar, och bristen har därmed höjts från gul till orange även om den inte fullt ut ägs lokalt av förvaltningen.

Arbetet med dataskydd är omfattande och genomgripande, men sammantaget har förvaltningen under 2023 påbörjat åtgärder som betydligt förbättrar förutsättningarna för 2024.

3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som nämnden, som är 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?	328
Har nödvändiga uppdateringar gjorts?	Ett omfattande arbete har skett men förteckningen är inte fullständig eller helt uppdaterad
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Rutiner har tagits fram men de behöver bli mer kända.

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.

Ett omfattande arbete har gjorts på avdelningarna, delvis med hjälp av en konsult, och 328 behandlingar var vid senaste kontroll (2023-12-27) registrerade i Draftit. Motsvarande siffra i 2022 års rapport var 74 behandlingar.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Omfattande uppdateringar har gjorts men förteckningen är inte helt uppdaterad.

DSO bedömer hur fullständig registerförteckningen är

Som framkommer ovan har stora förbättringar gjorts men registerförteckningen bedöms ännu inte vara fullständig.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Södermalms stadsdelsförvaltning har dataskyddsredogörare på varje avdelningen som ska registrera personuppgiftsbehandlingar och kontaktas vid behov av uppdatering eller ändring. De ska också skicka ut påminnelser till sina respektive avdelningar om uppdateringar. Från och med 2024 är tanken att de vid dessa tillfällen ska skicka ut standardiserade frågor för att underlätta för dem och cheferna samt för likställig hantering på alla avdelningar.

Rutinen, och framförallt att processägare måste kontakta dataskyddsredogörare när de ska påbörja en ny behandling eller uppdatera befintlig, behöver bli mer känd på förvaltningen. Rutinen kan göras känd på den återkommande utbildningen i

informationssäkerhet och dataskydd, på introduktion för chefer samt via påminnelser i nyhetsbrev.

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

3.1.5 DSO ger råd och rekommendationer till PUA

Såsom beskrivs ovan har förvaltningen gjort ett omfattande arbete registerförteckningen och stora förbättringar har skett.

Att brister ändå kvarstår beror på att registerförteckningen är så central för dataskyddet i stort, eftersom det är så PUA skaffar sig kännedom om personuppgiftsbehandlingar och risker kopplade till dessa.

PUA behöver nu förvalta det stora arbete som har gjorts genom att tillse dels att dataskyddsredogörarna fortsatt får bra förutsättningar att utföra sin uppgift, dels att förvaltningens processägare görs medvetna om att de ska kontakta dataskyddsredogörarna (och vid behov DSO) vid införande av nya eller ändring av befintliga arbetssätt som innebär behandling av personuppgifter.

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 i stort sett
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Vet ej
Är dokumenten uppdaterade?	Ja i stort
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja vad gäller lokala dokument

3.2.2 Syfte

Området syftar till att PUA genom styrdokument ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar PUA till medarbetare i sin verksamhet om vad som gäller och vad som förväntas av medarbetarna, när de hanterar personuppgifter. Att styrdokument finns nedtecknade, beslutade och kommunicerade medför att medarbetaren får dataskyddsinformation och kan behålla kunskapen över tid och tillämpa den på ett konsekvent sätt. En röd tråd i Dataskyddsförordningen är att viktiga arbetssätt och rutiner ska vara dokumenterade. Detta följer bland annat av kravet på att den personuppgiftsansvarige måste kunna visa att dataskyddsförordningens principer för behandling av personuppgifter efterlevs (artikel 5).

Rapporteringen av området är tvådelad: dels ska DSO bedöma om verksamheten har de styrdokument antagna och på plats, dels ska rapporteringen visa om dokumentationen innehållsmässigt håller en lämplig kvalitet, i vilket ingår bl.a. att dokumentationen ska vara uppdaterad och aktuell.

En brist inom detta område bör förstås ses som en brist i förhållande till direkta lagkrav, men det finns fler nyanser av detta som bör

lyftas fram till PUA. Bristande styrning på grund av att lämplig styrande dokumentation saknas leder exempelvis ofta till bristande kvalitet i hur verksamheten utför aktiviteterna, men även till att verksamheten slösar värdefulla resurser när exempelvis för många personer blir involverade i en incidenthantering eller för att en analys behöver göras om från grunden varje gång istället för att man återanvänder redan uppfunnen kunskap. Dessa effekter drabbar verksamheter ur ett vidare perspektiv och är något som ligger i PUA:s intresse att förstå för att fatta rätt beslut om.

Eftersom flera av styrdokumenten omfattar både dataskydd och informationssäkerhet bör DSO resonera med informationssäkerhetssamordnare i bedömningar och förslag på åtgärder framåt för nästa verksamhetsår.

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?

Lämplig styrande dokumentation finns på plats.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

DSO:s bedömning är att de centrala dokumenten i stort håller en lämplig kvalitet, är begripliga även för de som inte jobbar med dataskydd och ger ett tillräckligt stöd. När lokala styrdokument har tagits fram har DSO rådgjort med avdelningschef och vid behov kommunikatör för att dokumenten ska bli tillgängliga och pedagogiska. Om de upplevs så behöver dock granskas, och de behöver göras mer kända på förvaltningen.

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

3.2.5 DSO ger råd och rekommendationer till PUA

Den brist som anges är främst kopplad till att det ytterligare skulle behöva undersökas hur användarvänliga befintliga dokument är och att de behöver göras mer kända.

DSO avser därför att under 2024 göra en granskning av hur tillgängligheten upplevs, samt fortsätta att i ILS följa upp om och i så fall hur enheterna har gjort styrdokumenten 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?	49 (diarieförda)
Är klassade personuppgiftsbehandlingar aktuella?	Ja, förutom en (1).

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.

3.3.3 Resultat

I 2022 års rapport var antalet genomförda klassningar 38 vilket innebär att mer än 10 klassningar sedan dess har färdigställts. Under 2023 har även arbetet med att revidera och följa upp genomförda klassningar inletts. Samtliga informationsmängder som innehåller personuppgifter bedöms dock inte ha informationsklassats. Det finns också i nuläget brister i förutsättningarna att omhänderta de

åtgärder som identifieras i informationsklassningar kopplat till att förvaltningen inte har haft den rollbesättning som krävs för detta.

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

3.3.5 DSO ger råd och rekommendationer till PUA

För att samtliga av förvaltningens informationstillgångar ska bli klassade och tekniska och organisatoriska säkerhetsåtgärder därmed vidtagna och dokumenterade är det viktigt att förvaltningen fortsätter arbetet med att implementera PM3-modellen. Detta eftersom det behöver finnas ett tydligt ägarskap av processerna så att de åtgärder som identifierats kan implementeras och följas upp.

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. (Nej, eftersom inte alla behandlingar har identifierats så kan det potentiellt finnas högriskbehandlingar som inte konsekvensbedömts.)
Är de genomförda bedömningarna aktuella?	Ja

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 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.

3.4.2 Resultat

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

I samband med att arbetet med informationsklassningar har intensifierats genomförs även fler konsekvensbedömningar under 2023. DSO:s bedömning är dock att alla behandlingar som kräver en konsekvensbedömning inte har identifierats.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Nej.

Är de genomförda konsekvensbedömningarna aktuella?

DSO har skickat ut frågor för revidering av genomförda konsekvensbedömningar. Det har dock i flera fall varit svårt för verksamheterna att följa upp då inte rollerna objektägare och objektledare varit tillsatta.

3.4.3 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

3.4.4 DSO ger råd och rekommendationer till PUA

Rekommendationerna avseende konsekvensbedömningar är samma som de för informationsklassningar.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	Uppskattningsvis 4 kända
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	4. I ett (1) fall har dock PUA inte kunnat lämna information inom utsatt tid då informationen inte har erhållits av it-leverantörer.

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.)

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

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

Intetgritetsskyddsmyndighetens (”IMY”) sida, 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?

Förvaltningen har en lokal rutin på plats för att tillvarata registrerades rättigheter. Denna behöver dock bli mer känd. Att undersöka leverantörers förutsättningar för att till exempel sammanställa och radera information på begäran är en del av informationsklassningen.

När det gäller stadens it-leverantörer som också är personuppgiftsbiträden har dock brister upptäckts. Därav anges bristen som helhet relativt hög (se nedan), men då avtalen med it-leverantörerna ligger centralt är det inte en brist som förvaltningen äger.

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
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

3.5.5 DSO ger råd och rekommendationer till PUA

Den lokala rutinen för hantering av registrerades rättigheter behöver bli mer känd. Förvaltningen bör genom att genomföra informationsklassningar vid upphandlingar säkerställa att leverantörer man anlitar har förutsättningar att leva upp till registrerades rättigheter.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Rutinen är att misstanke om personuppgiftsincident omgående ska rapporteras till DSO. Det förekommer även att DSO vid regelbunden kontroll upptäcker händelser i IA som inte rapporterats som personuppgiftsincidenter, eller av en slump i polisanmälningar och Lex Sarah-rapporter.
Hur många personuppgiftsincidenter har dokumenterats?	27 2023-12-28 16:38.
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Till IMY: 16 Till berörda: 9 2023-12-28 16:38.
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	12 2023-12-28 16:38.

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 det förekomma många andra typer av incidenter, som inte involverar personuppgifter. Det är viktigt att hålla den saken i åtanke, så att årsrapporteringen inte omfattar annat än just personuppgiftsincidenter. Vidare är det en grundförutsättning för hanteringen av personuppgifter att incidenter över huvud taget upptäcks, samt att verksamheten förstår att hantera

incidenter som rör personuppgifter på det särskilda sätt som dataskyddsförordningen kräver.

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland dataskyddsförordningens olika verktyg för att åstadkomma en sund personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering. Stadens mall för DSO:s årsrapport är avsedd att fokusera på rapporteringen.

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

Bristande förmåga att rapportera personuppgiftsincidenter i tid kan leda till sanktioner från IMY:s sida. DSO:ns årsrapportering är därför avsedd att kartlägga detta, samtidigt som det finns möjlighet att redovisa vilka typer av personuppgiftsincidenter som inträffat, incidenternas allvarsgrad etc.

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

3.6.3 Resultat

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

Förmågan att rapportera personuppgiftsincidenter är överlag god och andelen incidenter som har rapporterats i tid är ungefär samma som 2022, då 18 av 21 incidenter som behövdes rapporteras till IMY rapporterades i tid.

Dock förekommer det fortfarande att händelser missas att rapporteras till DSO som just personuppgiftsincidenter, vilket i värsta fall kan få allvarliga konsekvenser i form av att PUA inte vidtar åtgärder för att informera och skydda den/de drabbade registrerade.

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

3.6.5 DSO ger råd och rekommendationer till PUA

Utöver obligatoriska webbutbildningar och återkommande lokal utbildning behöver förvaltningens chefer säkerställa att rutinen för att upptäcka och rapportera personuppgiftsincidenter är känd och att kunskap finns om att olika händelser, såsom inbrott, stöld av teknisk utrustning, ansökningshandlingar/akter som försvinner osv. också kan utgöra personuppgiftsincidenter och således behöva rapporteras separat parallellt med andra anmälningar såsom polisanmälningar, IA-anmälningar och Lex Sarah/Maria.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Styrdokument
- Personuppgiftsförteckning
- Tekniska och organisatoriska säkerhetsåtgärder
- Incidenter
- Konsekvensbedömningar

Som synes har Södermalms stadsdelsförvaltnings DSO valt att vid årets granskningar fokusera på de obligatoriska rapporteringsområdena.

4.2 Syfte

En av DSO:s 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.

4.3 Genomförda granskningar och deras resultat

Granskning 1

Se kapitel 3.2 samt SÖD 2023/704-1 Granskningsrapport styrdokument.

	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

Granskning 2

Under 2023 har förvaltningens registerförteckning granskats två gånger, i augusti och november. Mellan dessa två granskningar hade en stor förändring skett. Se bifogad sammanställning för november samt granskningsrapport SÖD 2023/704-2 för rapporten från augusti.

Se kapitel 3.1 i denna rapport för resonemang kring bedömningen av kvarstående brister.

	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

Granskning 3

Se kapitel 3.3 samt SÖD 2023/704-3 Granskningsrapport tekniska och organisatoriska 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

Granskning 4

Se kapitel 3.6 samt SÖD 2023/704-4 Granskningsrapport Personuppgiftsincidenter.

	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

Granskning 5

Se kapitel 3.4 samt SÖD 2023/704-5 Granskningsrapport Konsekvensbedömningar.

	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

4.4 DSO ger råd och rekommendationer till PUA

Råd och rekommendationer beskrivs under respektive stycke under kapitel 3, obligatoriska granskningsområden i denna rapport.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- PUA har inte tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar på plats
- PUA kan inte efterleva individens rättigheter
- PUA lämnar inte tillräcklig information till registrerade

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

Risk 1: PUA har inte tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar på plats

Möjligheten att få tekniska och organisatoriska skyddsåtgärder hänger ihop med att det finns en organisation med tydligt utsedda objektledare etc. som ansvarar för att ta in informationssäkerhets-inklusive dataskyddsaspekter från början vid nya arbetssätt, användning av ny teknik eller nya upphandlingar.

Då förvaltningen ännu inte fullt ut har en sådan organisation på plats finns en risk att dataskydd inte tas i beaktande och att tekniska och organisatoriska skyddsåtgärder därmed inte implementeras och följs upp.

	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

Risk 2: PUA kan inte efterleva individens rättigheter

För att förvaltningen ska kunna säkerställa registrerades rätt till information, rättelse och radering etc. behöver utöver befintlig lokal rutin stadens it-leverantörer kunna bistå förvaltningen och göra det inom den lagstadgade tidsramen. DSO har gjort observationer som tyder på att detta inte är fallet fullt. Detta är alltså inte en risk som förvaltningen äger fullt ut.

	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

Risk 3: PUA lämnar inte tillräcklig information till registrerade

Gemensamma blanketter med informationstexter om hur personuppgifter behandlas har tagits fram av bland andra social- och äldreförvaltningen. Dessa behöver dock ses över, vilket innebär att förvaltningen inte fullt ut äger denna risk. Som personuppgiftsansvarig måste dock förvaltningen ändå regelbundet se över vilken information om personuppgiftsbehandling som lämnas till registrerade.

	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

5.4 DSO ger råd och rekommendationer till PUA

Se rekommendationer för respektive risk under kapitel 3.

Risk 3, PUA lämnar inte tillräcklig information till registrerade, ägs bara delvis av förvaltningen då många av de informationstexter som används på ansökningsblanketter och liknande är framtagna centralt. DSO fortsätter att lyfta frågan i sitt nätverk, men förvaltningens enheter behöver se över vilken information som lämnas i de processer där personuppgifter behandlas.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Information till registrerade
- Uppgifts- och lagringsminimering

6.2 Syfte

Som nämnts ovan är det granskande arbetet en av DSO:s viktigaste uppgifter. 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

Granskning 1: Information till registrerade

Utifrån den risk som har identifierats i denna rapport kommer DSO att fortsätta dialogen med andra DSO:s, framförallt på social- och äldreförvaltningen för att se över möjligheten för dem att lyfta frågan på sina förvaltningar om att uppdatera centrala blanketter vid behov. DSO kommer även under året att granska vilken information förvaltningen som personuppgiftsansvarig lämnar till registrerade.

Granskning 2: Uppgifts- och lagringsminimering

Uppgiftsminimering, att inte behandla fler personuppgifter än vad som är nödvändigt för syftet, och lagringsminimering, att inte spara personuppgifter längre tid än stadens hanteringsanvisningar säger, är två så kallade allmänna dataskyddsprinciper. Även om laglig grund finns för behandlingen behöver dessa principer uppfyllas för att behandlingen som helhet ska vara laglig.

DSO kommer därför att granska hur väl förvaltningen uppfyller principerna.

Utöver detta kommer de obligatoriska rapporteringsområdena som beskrivs i kapitel 3 i denna rapport granskas. Särskilt fokus kommer att ligga på tekniska och organisatoriska skyddsåtgärder, som ju som beskrivs ovan, är sammankopplat med den personuppgiftsansvarigas arbete med informationsklassningar och konsekvensbedömningar vid nya upphandlingar och arbetssätt.