Stockholms stad

Bilaga 03

GDPR Årsrapport

År 2022

Södermalms stadsdelsnämnd

GDPR årsrapport
December 2022
Dnr: SÖD 2022/1136
Utgivningsdatum: 2023-02-23
Kontaktperson: Anna Remmets

1 Bakgrund

Dataskyddsförordningen (GDPR) 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. GDPR syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

Enligt GDPR 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 GDPR 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 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 (PUA) efterlever dataskyddslagstiftningen.

GDPR bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnd eller bolagsstyrelse ska kunna *visa* att verksamheten efterlever GDPR. 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.

Södermalms stadsdelsnämnd bedöms i nuläget inte ha några brister eller risker på den högsta, röda, nivån. I de flesta granskningsområdena har brister identifierats ”som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga”. Att det ändå har identifierats brister inom samtliga granskningsområden kan till stor del antas ha att göra med att Dataskyddsförordningen (GDPR) fortfarande är en relativt ny lagstiftning som kräver nya och omfattande arbetssätt. Då GDPR ställer höga krav är den lägsta bristnivån ”Inga brister av nämnvärd betydelse identifierade” svår att uppnå.

I de fall då till och med en större brist inom samma granskningsområde än vid föregående år har identifierats betyder inte det att förvaltningen blivit *sämre.* Det kan istället handla om nya analyser, domar etc. inom området gör att DSO landat i en annan slutsats. I granskningen av information till registrerade bedömer till exempel DSO att vissa av de stadsgemensamma blanketter som tagits fram centralt i staden som används inte helt uppfyller informationskravet, vilket varit DSO:s bedömning tidigare men kommit att omprövas när mer kunskap om vad GDPR:s informationskrav innebär har blivit tillgänglig.

Sammanfattningsvis finns de största bristerna, och därmed riskerna i förvaltningens arbete med personuppgiftsförteckning och konsekvensbedömning. Inom båda områdena har ett relativt intensivt arbete pågått under 2022 och en viss förbättring har skett, men eftersom de är så centrala för att förvaltningen ska kunna leva upp till GDPR:s krav identifieras bristen fortfarande som relativt stor och är även till stor del upphov till de risker som beskrivs i stycke 5.

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 (GDPR) 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 Dataskyddsombudets (DSO:s) slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:s genomförda uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	384
Har nödvändiga uppdateringar gjorts?	Vissa, men inte tillräckligt
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Det arbetssätt som beslutas fungerar inte fullt ut.

3.1.2 Syfte

Det följer av (GDPR) (artikel 30) att stadens alla förvaltningar och bolag måste inventera alla personuppgifter som behandlas i verksamheten, både i rollen som PUA 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. Att ha en registerförteckning på plats leder till att verksamheten kan arbeta mer resurs- och kostnadseffektivt med sitt systematiska och riskbaserade dataskyddsarbete.

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 samt 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

Under 2022 har arbetssättet med dataskyddsredogörare på varje avdelning testats. Uppgiften har tidigare av förvaltningsledningen beslutats omfatta 10 procent av en heltidstjänst och huvuduppdraget är att uppdatera förvaltningens personuppgiftsförteckning utifrån underlag från de respektive avdelningarna.

Arbetssättet har hittills inte fungerat optimalt då det har varit svårt för dataskyddsredogörarna och deras chefer att viga tillräckligt med tid och skapa rutiner för att informera dem om nya/förändrade personuppgiftsbehandlingar inte verkar ha upprättats på avdelningarna.

Antalet registrerade behandlingar har dock ökat något även om registerförteckningen fortfarande inte är fullständig och de registrerade behandlingarna är ojämnt fördelade över avdelningarna (se Granskningsrapport 1 och 4, SÖD 2022/810-1 och 810-4).

DSO kontrollerar hur många behandlingar som registrerats

Ur granskningsrapport 4, SÖD 2022/810-4:

Avdelning	**Antal personuppgifts-behandlingar införda i Draftit**	**Behandlingar i tidigare inlämnade inte förts in i Draftit**
Sociala avdelningen	8 (Granskningsrapport 1: 8)	113
Äldreomsorgsavdelningen	2 (Granskningsrapport 1: 2)	120
Förskoleavdelningen	2 (Granskningsrapport 1: 2)	61
Stadsmiljöavdelningen	3 (Granskningsrapport 1: 3)	0
Ekonomiavdelningen	19 (Granskningsrapport 1: 18)	11
HR-avdelningen	15 (Granskningsrapport 1: 13)	1
Avdelningen Stab och kansli	25 (Granskningsrapport 1: 8)	4

DSO kontrollerar om nödvändiga uppdateringar gjorts
Antalet registrerade personuppgiftsbehandlingar har ökat med ca 70 st under 2022. Rutinerna att informera dataskyddsredogörarna om nya behandlingar tycks dock brista. Dataskyddsredogörarna upplever vidare att det är svårt att avsätta den beslutade tiden och att verktyget Draftit är komplicerat.

DSO bedömer hur fullständig registerförteckningen är

Förteckningen bedöms inte vara fullständig på någon av avdelningarna. Antalet registreringar är ojämnt fördelat över avdelningarna och sociala avdelningen, som kan antas ha ett stort antal känsliga behandlingar har registrerat relativt få behandlingar i Draftit. Fler finns i de tidigare ifyllda excelfilerna, men dessa är nu flera år gamla.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Se ovan.

3.1.4 DSO anger hur allvarliga bristerna är på en skala

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

3.1.5 DSO ger råd och rekommendationer till PUA

Arbetssättet med dataskyddsredogörare fungerar för de flesta avdelningar inte optimalt i praktiken då det är svårt att få till rätt förutsättningar framförallt vad gäller tidsåtgång.

Att ha dataskyddsredogörare som förtecknar förvaltningens personuppgiftsbehandlingar är *ett* arbetssätt, och det finns alla möjligheter att testa andra. De grundförutsättningar som är viktiga att ha med sig är dock:

- Att ha en uppdaterad personuppgiftsförteckning som är ett ”levande dokument” är en centralt för att kunna efterleva (GDPR).
- Redovisningen av förvaltningens personuppgiftsbehandlingar måste göras av de som äger och har kännedom om de olika processerna. Detta innebär dock inte nödvändigtvis att samma personer behöver registrera dem i systemstödet Draftit.
- DSO har en granskande och rådgivande roll, vilket innebär att DSO ska granska personuppgiftsförteckningen och alltså inte själv bör arbete med denna operativt, men kan ge stöd i den mån det behövs.

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?	Kan förbättras
Är dokumenten uppdaterade?	Behöver ses över
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. 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 (GDPR) är att viktiga arbetssätt och rutiner ska vara dokumenterade. Detta följer bland annat av kravet på att PUA måste kunna visa att GDPR:s principer för behandling av personuppgifter efterlevs (artikel 5).

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?
Ja, centrala dokument och rutinbeskrivningar har tagits fram för alla centrala processer.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet
I stort sett, men det har förekommit att uppdatering har släpat efter något. Vissa dokument behöver också omarbetas och förenklas i lokala dokument.

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

Chefer bör se till att medarbetare på förvaltningen känner till och vid behov kan söka relevant information på stadens centrala sida om dataskydd, https://intranat.stockholm.se/Sidor/2019/2/Nya-Dataskyddsforordningen-GDPR-/.

DSO kommer under 2023 se över behovet av lokala dokument.

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?	38 (2022-12-05)
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. Notera att enbart sådan informationsklassning som avser behandling eller system som omfattar personuppgifter är av intresse för DSO:s årsrapportering. Förvaltningens informationssäkerhetssamordnare (ISAM) finns som stöd i detta arbete.

3.3.3 Resultat

Under 2022 har ett intensivt arbete med att klassa nämndens informationstillgångar pågått. Detta har lett till ett betydligt bättre läge i jämförelse med föregående år. Alla informationstillgångar är dock ännu inte klassade.

3.3.4 DSO anger hur allvarliga bristerna är på en skala

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

3.3.5 DSO ger råd och rekommendationer till PUA

Rutiner så att processägare själva kan initiera eller flagga upp behovet av informationsklassningar behöver förbättras på enheterna. Chefer bör säkerställa att de nya tillämpningsanvisningarna för informationssäkerhet som finns är kända.

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 GDPR. 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?

I och med det intensiva arbetet med informationsklassningar har också behov av konsekvensbedömningar identifierats och genomförts. Troligtvis är dock inte alla behandlingar identifierade.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Flera högriskbehandlingar har konsekvensbedömts i samband med informationsklassningar, men med största sannolikhet har alla ännu inte konsekvensbedömts.

Är de genomförda konsekvensbedömningarna aktuella?
Ja.

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
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

3.4.5 DSO ger råd och rekommendationer till PUA

Det behöver finnas rutiner på enheterna så att processägarna vet att de ska kontakta ISAM och DSO vid nya upphandlingar eller arbetssätt där informationsklassning och konsekvensbedömning kan behövas. ISAM och DSO är behjälpliga genom processen, men den måste initieras av de som har kännedom om nya upphandlingar/arbetssätt. DSO har tagit fram en rutin som kan användas (bilaga 1).

För att kunna identifiera högriskbehandlingar är det också nödvändigt att personuppgiftsförteckningen hålls uppdaterad och aktuell.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	1
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	Ej känt

3.5.2 Syfte

Registrerade personer har enligt GDPR (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 PUA – dvs. i stadens fall nämnder och bolag – tillgodoser rättigheterna i fråga.

Rättigheterna medför att registrerade personer kan 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 GDPR:s 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.)

Om verksamheten inte klarar av att hantera en begäran från en registrerad person i enlighet med GDPR:s krav, kan det skada allmänhetens förtroende för hur staden hanterar personuppgifter. Det kan även leda till tillsynsärenden från Integritetsskyddsmyndighetens (IMY) sida, med sanktioner som följd.

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

DSO informerar kontinuerligt vid bland annat utbildningar om registrerades rättigheter. Den stadsövergripande rutin som finns verkar dock vara relativt okänd och DSO har fått signaler om att den upplevs som svårtillgänglig. En kontakt med en enskild som vänt sig till DSO har visat på en möjlig brist i hanteringen hos enheten ifråga.

Förfrågningarna från enskilda är av allt att döma få. Då få förfrågningar inkommer påminns inte heller medarbetare och chefer om den befintliga rutinen för att tillgodose registrerades rättigheter.

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

3.5.5 DSO ger råd och rekommendationer till PUA

DSO ska ta fram en lokal rutin för att tillgodose den registrerades rättigheter. Därefter kommer DSO att be cheferna att göra denna känd för medarbetare. Detta kan till exempel ske genom att DSO bjuds in till APT eller liknande.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	De flesta genom att den som upptäckt incidenten meddelar DSO. En del upptäcks av DSO i samband med kontroll i incidentrapporteringssystemet IA. Det har förekommit att de upptäckts via polisrapporter om stöld eller att händelsen rapporterats som en Lex Sarah.
Hur många personuppgiftsincidenter har dokumenterats?	31
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	21 till IMY. 9 till de registrerade.
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	18

3.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt GDPR (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.” Det är en grundförutsättning för hanteringen av personuppgifter att incidenter upptäcks, samt att verksamheten förstår att hantera incidenter som rör personuppgifter på det särskilda sätt som GDPR kräver.

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland GDPR:s 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. GDPR 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 GDPR 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 GDPR 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 incidenter är relativt god. En indikation på detta är att flera olika personer inom olika verksamhetsområden självmant vänder sig till förvaltningens DSO när de misstänker att en incident har inträffat. Av de 21 incidenter som rapporterats till IMY är det endast 3 som rapporterats för sent.

Att incidenter som fortfarande inte kommit till DSO:s kännedom istället upptäcks i till exempel polisanmälningar och IA- och Lex Sarah-rapporter (om än inte i någon hög grad) tyder det på att det fortfarande finns kunskapsbrister om hur och när personuppgiftsincidenter ska rapporteras. Som synes är antalet incidenter där verksamheten har angett att man informerat eller avser informera de enskilda relativt lågt i förhållande till det antal incidenter som ansetts vara så pass allvarliga att de behövts

rapporteras till IMY. DSO informerar alltid vid incident om att utgångspunkten ska vara transparens. Verksamheterna kan dock göra bedömningen att deras klienter av olika anledningar skulle lida större men av informationen än av incidenten som sådan eller inte ha förmåga att ta till sig informationen. I ett par fall har den enskilda redan varit medveten om incidenten.

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

Alla medarbetare och chefer ska gå den obligatoriska webutbildningen i dataskydd och uppmanas att gå de återkommande utbildningar som DSO och ISAM håller i. I information och instruktioner för rapportering av IA och Lex Sarah samt för polisanmälningar bör information finnas med om att händelsen om den rör personuppgifter som kan ha röjts, ändrats, eller förstörts ska rapporteras till förvaltningens DSO.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Personuppgiftsförteckningen (två granskningar)
- Information till registrerade
- Konsekvensbedömningar

4.2 Syfte

En av dataskyddsombudets (DSO:s) viktigaste uppgifter är att övervaka verksamhetens efterlevnad av dataskyddsförordningen (GDPR). En central del av det arbetet är att göra återkommande granskningar av hur väl GDPR efterlevs. Resultaten av granskningarna påverkar i stor utsträckning vilka beslut verksamheten kan fatta i fråga om dataskyddsåtgärder. För personuppgiftsansvarig (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

Personuppgiftsförteckningen

Se stycke 3.1

Information till registrerade

GDPR fastslår att PUA ska vara transparent gentemot de registrerade (de vars personuppgifter PUA behandlar). Den registrerade ska kunna förstå att och varför hens personuppgifter behandlas, samt få information om vart hen kan vända sig för att få mer information eller göra invändningar.

Granskningen av förvaltningens information till registrerade beskrivs närmare i Granskningsrapport 2. Förvaltningens enheter och verksamheter använder sig till stor del av de stadsgemensamma blanketter som tagits fram av socialförvaltningen,

äldreförvaltningen och serviceförvaltningen. Vid granskningen av dessa föreföll dock inte informationen alltid leva upp till GDPR:s informationskrav, och DSO har därför inlett en dialog med dessa fackförvaltningar.

	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

Konsekvensbedömningar
Se stycke 3.4.

4.4 DSO ger råd och rekommendationer till PUA

Personuppgiftsförteckningen
Se stycke 3.1.

Information till registrerade
Chefer på förvaltningen behöver säkerställa att informationskravet uppfylls vid kontakter med enskilda som leder till att deras personuppgifter samlas in och sparas en längre eller kortare tid även när kontakten inte leder till någon ansökan. De behöver också säkerställa att uppdaterade centrala blanketter används. DSO har tagit fram ett PM om skillnaden mellan information och samtycke som bör spridas på enheterna.

Konsekvensbedömningar
Se stycke 3.4.

5 Risker inom dataskydd

5.1 Sammanfattning
Relevanta risker inom verksamheten:

- Den personuppgiftsansvariga (PUA) har inte fullständig överblick över sina personuppgiftsbehandlingar.
- Dataskydd tas inte i beaktande vid upphandlingar, införanden av nya system eller arbetssätt.

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 (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 fullständig överblick över sina personuppgiftsbehandlingar.

Kännedom om och överblick över sina personuppgiftsbehandlingar är en förutsättning för att kunna ge personuppgifter nödvändigt skydd och identifiera risker. Denna överblick skaffar sig PUA genom att upprätta och regelbundet uppdatera en förteckning över sina personuppgiftsbehandlingar, en så kallad personuppgifts- eller registerförteckning.

Södermalms stadsdelsförvaltning har under 2022 arbetat med dataskyddsredogörare som ska föra in dessa förteckningar i systemet Draftit. Inom vissa avdelningar har en påtaglig förbättring skett medan arbetet inte har gått framåt inom andra (se stycke 3.1).

Förvaltningen som helhet bedöms därför inte ha en fullständig förteckning, och därmed inte en fullständig överblick över sina personuppgiftsbehandlingar.

	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: Dataskydd tas inte i beaktande vid upphandlingar, införanden av nya system eller arbetssätt.

För att vara säker på att bestämmelserna i GDPR följs behöver den PUA ta dataskydd i beaktande innan en ny upphandling eller införande av nytt system, ny teknik eller arbetssätt. Även i de fall då förvaltningen använder sig av tekniska lösningar som upphandlats och införts centralt behöver förvaltningen göra en egen analys (men gärna i samverkan med och underlag från SLK och andra förvaltningar) av dataskydd och informationssäkerhet. Om en inledande analys visar att en process kommer innebära höga risker för de registrerades integritet ska en konsekvensbedömning göras.

Under 2022 har förvaltningens informationssäkerhetssamordnare (ISAM) tillsammans med DSO arbetat intensivt med att genomföra informationsklassningar och konsekvensbedömningar och även tagit fram en tillämpningsanvisning för informationssäkerhet (där dataskydd ingår). ISAM och DSO har även hållit utbildningar i olika forum.

Det finns dock fortfarande kunskapsbrister om hur dataskydd säkerställs inför nya upphandlingar och arbetssätt, vilket visas av bland annat resultatet av granskningen av genomförda konsekvensbedömningar (se stycke 3.4).

	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

Att ha överblick över sina personuppgiftsbehandlingar och att ta dataskydd i beaktande innan nya processer påbörjas kan beskrivas som ett ”skelett” som resten av dataskyddsarbetet hänger på.

Att få arbetet med personuppgiftsförteckningen att fungera behöver därför vara en prioriterad fråga inom dataskydd. Exakt med vilka metoder detta ska ske kan avdelnings- eller enhetschefer resonera kring tillsammans med DSO.

Förvaltningens ISAM har tillsammans med DSO under 2022 arbetat intensivt med informationsklassningar och konsekvensbedömningar, vilket kan antas ha ökat kännedomen på förvaltningen om att informationssäkerhet, inklusive dataskydd, måste tas med inför att ett nytt arbetssätt påbörjas eller ny teknisk lösning tas i bruk. Den nya tillämpningsanvisningen för informationssäkerhet samt rutinbeskrivningen inför upphandling/införande behöver dock göras kända på lämpligt sätt.

Chefer behöver säkerställa att medarbetare går de obligatoriska webbutbildningarna i informationssäkerhet och dataskydd och uppmuntra dem att gå på de utbildningar som DSO och ISAM håller en gång per termin.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Personuppgiftsförteckningen
- Konsekvensbedömningar

6.2 Syfte

Det granskande arbetet är en av dataskyddsombudets (DSO:s) viktigaste uppgifter. Granskningsområdena väljs utifrån ett riskbaserat synsätt, det vill säga att fokus ska 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 tillräcklig nivå.

6.3 Planerade granskningar

Granskning 1: Personuppgiftsförteckningen

Då en risk (se stycke 5) är att förvaltningen inte har fullständig överblick över sina personuppgiftsbehandlingar och en korrekt och uppdaterad personuppgiftsförteckning är en grundförutsättning för att kunna leva upp till bestämmelserna i dataskyddsförordningen (GDPR), kommer personuppgiftsförteckningen vara ett prioriterat granskningsområde även under 2023.

Granskning 2: Konsekvensbedömningar

Att vid behov genomföra konsekvensbedömningar innan ett nytt system/arbetssätt tas i bruk är en annan förutsättning för att kunna identifiera och åtgärda risker och därmed leva upp till bestämmelserna i GDPR.

7 Övrigt att rapportera

Ett stort och stadsövergripande problem för dataskyddet är att det hittills inte har gått att mejla på ett helt säkert sätt. Detta då stadens interna mejl är skyddad vid överföringen men inte när den ligger i någon av Outlookkorgarna. För de medarbetare som har Fujitsuleveransen finns inget sådant skydd.

Den lösning som staden har tagit fram är Säkra Meddelanden (Trusted Dialog) som gör så att man kan skicka mejl utan risk för att röja sekretess eller bryta mot GDPR. Tjänsten är möjlig att ladda ner redan nu, men rekommendationen är att den inte ska användas förrän förvaltningarna lokalt har gjort informationsklassningar och konsekvensbedömningar. Dessa har genomförts på Södermalms stadsdelsförvaltning, men det kvarstår fortfarande tekniska frågor där svar inväntas från stadsledningskontoret och produktleverantören innan informationssäkerhetssamordnaren och dataskyddsombudet kan rekommendera att tjänsten börjar användas.