Stockholms stad

Bilaga 10

GDPR Årsrapport

År 2023

Skarpnäcks stadsdelsnämnd

GDPR årsrapport
Januari 2024

Dnr: 2024/20
Utgivningsdatum: 2024-01-11
Kontaktperson: Julia Ögren, dataskyddsombud

1 Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

Enligt dataskyddsförordningen är varje nämnd och bolagsstyrelse inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnd och bolagsstyrelse behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett Dataskyddsombud (”DSO”). DSO:n har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är således ett medel för nämnd och styrelse att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnd eller bolagsstyrelse ska kunna *visa* att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna *dokumenteringsskyldighe*t. Årsrapporten är även ett medel för nämnds/bolagsstyrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehåll

2 Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

Under tidig höst 2023 har arbetet för att nå en översiktsbild av förvaltningens dataskyddsarbete i syfte att rekommendera prioriterade åtgärder till förvaltningsledningen intensifierats.

I samband med denna kartläggning har det identifierats omfattande brister avseende registerförteckningen vilket lett till slutsatsen att registret som helhet inte på ett korrekt sätt återspeglar de personuppgiftsbehandlingar som sker inom förvaltningen. Allvarliga brister har identifierats när det kommer till den mycket låga förekomsten av konsekvensbedömningar och informationsklassningar. Dessa områden är delar i dataskyddsarbetet som syftar till att säkerställa att adekvata skyddsåtgärder tillämpas för personuppgiftsbehandlingar, särskilt sådana som innebär hög risk för personers fri- och rättigheter. Kunskapsläget både bland medarbetare och chefer bedöms fortfarande vara lägre än önskvärt vilket i sig leder till lägre efterlevnad av dataskyddsförordningens regler. Mot bakgrund av detta nuläge har ett arbete påbörjats under hösten för att stärka kunskaper i dataskyddsfrågor. Utbildning i GDPR och presentation av föreslagna åtgärder gällande förvaltningens organisation kring dataskydd har getts till förvaltningsledning och under chefsforum, och sammanlagt sex utbildningstillfällen har erbjudits till dataskyddssamordnare och chefer både gällande GDPR och registrering i Draftit Privacy Records under 2023. Rollen personuppgiftsredogörare som beskrevs i GDPR årsrapport 2021 har vidareutvecklats till dataskyddssamordnare för att skapa en bredare och mer hållbar organisation i dataskyddsfrågorna.

Viktiga steg har tagits för att stärka stadsdelen i dataskyddsarbetet, förutom utbildningstillfällen så har en handbok och rutiner för personuppgiftsincidenthantering samt inventering och registrering av personuppgiftsbehandlingar beslutats och publicerats. I väntan på att fler lokala rutiner tas fram rekommenderas att ledning och verksamheter tar del av stadsgemensamma rekommendationer och rutiner i de delar som saknas.

Centralt för ett fortsatt framgångsrikt dataskyddsarbete är att arbeta för att skapa systematik och att integrera dataskyddet i det dagliga arbetet, samt att arbetet leds och prioriteras av förvaltningens ledning och övriga chefer.

3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som Personuppgiftsansvarig (”PUA”) som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som dataskyddsförordningen avser.

De obligatoriska rapporteringsområdena är registerförteckning, styrdokument, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, konsekvensbedömningar, individens rättigheter och personuppgiftsincidenter.

Nedan redogörs för nämndens eller bolagets status och DSO:ns slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:ns genomförda uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	111
Har nödvändiga uppdateringar gjorts?	Nej
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Nej

3.1.2 Syfte

Det följer i klartext av artikel 30 dataskyddsförordningen att stadens alla förvaltningar och bolag måste inventera alla personuppgifter som behandlas i verksamheten, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde, och dokumentera dem i en så kallad registerförteckning (även kallat behandlingsregister).

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

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

Eftersom inventeringen av personuppgifter i sig är avgörande för allt det fortsatta dataskyddsarbetet inom verksamheten, är denna

lägesbild en av de viktigaste slutsatserna som PUA behöver förstå och ta ställning till inför det planerade åtgärdsarbetet under nästa verksamhetsår.

3.1.3 Resultat

Det finns idag 111 registreringar upptagna i Draftit Privacy Records (registerförteckningen) för Skarpnäcks stadsdelsförvaltning. Det är enbart dessa registreringar som ligger till grund för bedömningen.

Majoriteten av dessa registreringar, 65 %, har inte uppdaterats sedan 2019-2020 och många av registreringarna har gjorts av personer som inte längre arbetar i förvaltningen. Det behöver inte betyda att de befintliga registreringarna inte fortsatt stämmer till del, men det går heller inte att avgöra om så är fallet. Det kan inte sägas att nödvändiga uppdateringar har gjorts eftersom deras innehåll och aktualitet inte har kontrollerats av verksamheterna under denna period. Det kan också konstaterats att vissa verksamheter som behandlar personuppgifter i stor skala enbart har ett fåtal behandlingar upptagna i registret medan andra saknar registreringar helt. Det kan utifrån bristen på uppdateringar och avsaknaden av registreringar därmed konstateras att registerförteckningen inte är att anses som komplett.

En annan brist är att det för majoriteten av registreringarna inte angetts någon risknivå på själva behandlingen. Det blir därför svårt att överblicka och prioritera skyddsåtgärder.

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

Utifrån ovan resultat görs den sammanvägda bedömningen att registerförteckningen har omfattande brister som kräver omgående åtgärder från ledning och verksamheter.

3.1.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet har under hösten föreslagit för förvaltningsledningen att verksamheterna ska utse dataskyddssamordnare som bland annat kan stötta i registreringen.

Utbildningar har erbjudits till både dataskyddssamordnare och chefer under senhösten 2023 gällande registerförteckningen och planerade tillfällen har även aviserats för 2024. Rekommendationen är att följa upp de verksamheter som fortfarande inte utsett dataskyddssamordnare och se till att det finns en organisation och planering kring registerförteckningen i varje del av förvaltningen samt att chefer och dataskyddssamordnare genomför och efterfrågar utbildningar i den mån de anser sig i behov av detta. Det rekommenderas även att följa upp huruvida dataskyddssamordnarna anser sig ha tillräckligt med kunskap och övriga resurser för att bistå cheferna i arbetet med registerförteckningen.

En lokal rutin gällande inventering och registrering har publicerats i december och rekommendation ges att sprida denna och implementera arbetssättet i verksamheterna.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Delvis, fler rutiner behöver tas fram
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Ja
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Ja
Är dokumenten uppdaterade?	Ja
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja

3.2.2 Syfte

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

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

Att styrdokument finns nedtecknade, beslutade och kommunicerade medför att medarbetaren får dataskyddsinformation och kan behålla kunskapen över tid och tillämpa den på ett konsekvent sätt. En röd tråd i dataskyddsarbetet är att viktiga arbetssätt och rutiner ska vara dokumenterade. Detta följer bland annat av kravet på att PUA måste kunna visa att principer för behandling av personuppgifter efterlevs (artikel 5).

3.2.3 Resultat

Förvaltningen har saknat beslutade och kommunicerade styrdokument för dataskyddsarbetet. Under hösten 2023 år har därför ett arbete gjorts för att ta fram styrdokument. Framtagandet av dessa dokument har skett genom att ta del av goda exempel från andra förvaltningar, ta del av relevant vägledning från exempelvis Integritetsskyddsmyndigheten och stadens centrala dokument. Styrdokumenten har även skickats till en referensgrupp som har getts möjlighet att inkomma med synpunkter, detta för att förankra rutiner tidigt i verksamheterna. Styrdokumenten som publicerats i december är Handbok för hanteringen av personuppgifter enligt dataskyddsförordningen, Rutin för hanteringen av personuppgiftsincidenter och rutin för inventering och registrering i Draftit Privacy Records.

Det saknas fortfarande styrdokument/rutiner för exempelvis att tillgodose individers rättigheter, konsekvensbedömning och gallring.

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

Rekommendationen är att under 2024 ta fram fler rutiner för att stödja verksamheterna i sitt dataskyddsarbete. Att ta fram rutiner för hur verksamheterna tillgodoser individers rättigheter kan med fördel prioriteras, men också vägledning kring konsekvensbedömningar och gallringsrutiner.

I övrigt bör det övervägas hur framtagandet av rutindokument kan ske på ett sätt där dataskyddsombudet får mer rådgivande än ledande roll i arbetet, detta för att förbättra förutsättningarna för dataskyddsombudets oberoende granskning av området framöver.

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?	Två system har klassats och i dessa behandlas personuppgifter. Enskilda personuppgiftsbehandlingar har inte klassats.
Är klassade personuppgiftsbehandlingar aktuella?	Den klassning av system som skett bedöms aktuell.

3.3.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd så ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA.

Utan informationsklassningen har verksamheten inte förutsättningar att välja rätt åtgärder för att skydda sin information och därmed leva upp till kraven i dataskyddsförordningen. Det är därför av stor betydelse för dataskyddsarbetet att PUA ges en uppdaterad bild varje år av huruvida informationsklassning är genomförd för personuppgifter som verksamheten hanterar. Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare.

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

3.3.3 Resultat

Förvaltningen saknar informationsklassningar med få undantag. Ur ett personuppgiftsperspektiv betyder det att det i stort saknas förutsättningar för förvaltningen att säkerställa att rätt åtgärder vidtas för att uppnå adekvat skyddsnivå i enlighet med dataskyddsförordningens krav för de personuppgiftsbehandlingarna som sker.

Under 2023 har dock steg tagits för att ta fram en plan och prioritering när det kommer till genomförandet av informationsklassningar där förvaltningen tagit hjälp av extern konsult. I närtid är det planerat för två normerande klassningar i staden, där förvaltningen kommer att vara representerade men också ta del av resultaten för att genomföra lokala klassningar utifrån resultaten.

3.3.4 DSO anger hur allvarliga bristerna är på en skala

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

	Inga brister av nämnvärd betydelse identifierade

Utifrån dagsläget där förvaltningen enbart har två informationstillgångar klassade kan bristerna inte beskrivas på annat sätt än allvarliga och att de omgående kräver insatser från ledning och verksamheter.

3.3.5 DSO ger råd och rekommendationer till PUA

För att personuppgifter ska kunna hållas skyddade och personuppgiftsbehandlingar ske på ett lagenligt sätt så behöver tekniska och organisatoriska skyddsåtgärder prioriteras.

Rekommendationen är även att ta ett helhetsperspektiv på hur resurser ska tillsättas för att uppnå detta. Kartläggningen av informationstillgångar behöver ske för att prioriteringen ska ske på rätt sätt. Ur ett personuppgiftsperspektiv är det viktigt att arbeta på ett riskbaserat sätt, det vill säga att prioritera de personuppgiftsbehandlingar och informationstillgångar som behandlar känsligast information först.

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. En konsekvensbedömning har till syfte att identifiera och dokumentera

risker kopplade till en viss behandling, samt att bedöma sannolikheten och konsekvensen om riskscenariot skulle inträffa. Baserat på bedömningen vidtas förebyggande åtgärder.

Konsekvensbedömningen anses liksom registerförteckning och informationsklassning som ett viktigt verktyg för verksamhetens dataskyddsarbete. Kravet på konsekvensbedömning är dessutom ett uttryckligt krav enligt dataskyddsförordningen. och ska utföras för alla behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1), vilket alltså syftar på risken för personers integritet. Dataskyddsförordningens krav på konsekvensbedömning gäller oavsett om behandlingen redan existerade eller inte när dataskyddsförordningen trädde ikraft.

3.4.3 Resultat

Förekomsten av konsekvensbedömningar har kontrollerats i diariet, i samtal med ledning och kontroll i registerförteckningen. Det kan konstateras att förvaltningen, med ett undantag från 2021, saknar konsekvensbedömningar. Den konsekvensbedömning som är gjord bedöms fortsatt vara relevant.

Mot bakgrund av detta kan det inte sägas att man identifierat alla behandlingar som det borde göras konsekvensbedömningar av.

3.4.4 DSO anger hur allvarliga bristerna är på en skala

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

Då förvaltningen saknar konsekvensbedömningar för behandlingar som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ges inget utrymme att göra annan bedömning än att det finns allvarliga brister som omgående kräver insatser av ledning och övriga verksamheten på detta område.

3.4.5 DSO ger råd och rekommendationer till PUA

Ledning och verksamheter behöver se helheten och kopplingen mellan registerförteckningen, riskanalys och

konsekvensbedömning. I ordning kan det betyda att inventera behandlingar i registerförteckningen och där ange risknivå för de olika behandlingarna, göra en riskanalys över de behandlingar som sker i verksamheterna och därifrån gå vidare med att genomföra konsekvensbedömningar för samtliga behandlingar som bedöms utgöra högriskbehandlingar.

I frågeställningen huruvida en konsekvensbedömning bör göras eller ej så bör verksamheterna förutom att ta del av stadsgemensamma riktlinjer titta på Integritetsskyddsmyndighetens hemsida där förteckning finns över situationer där konsekvensbedömning blir aktuellt, samt konsultera dataskyddsombudet.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	0
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	N/A

3.5.2 Syfte

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

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

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

3.5.3 Resultat

Tidigare år har förfrågan om registerutdrag hanterats inom föreskriven tid. I år har inga sådana begäran inkommit till stadsdelen.

Förutsättningar att hantera registrerades rättigheter torde i stor utsträckning bero på vilken kunskap som verksamheterna har om de registrerades rättigheter och det stöd i form av rutiner och styrdokument som finns att tillgå. Det saknas underlag för att bedöma detta granskningsområde utifrån faktiska begäran, men avsaknaden av rutin för att tillgodose registrerades rättigheter och att större utbildningsinsatser (förutom den obligatoriska grundutbildningen som årligen ska genomföras) kan ge en indikation om hur förutsättningarna ser ut idag.

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

Bristerna på detta område behöver åtgärder eftersom de i stort härleds till den generella kunskapsnivån samt avsaknaden av lokala rutiner om hur förvaltningen tillgodoser individers rättigheter. Bristen bedöms dock inte vara allvarliga eller brådskande.

3.5.5 DSO ger råd och rekommendationer till PUA

PUA föreslås ta fram lokala rutiner för hur förvaltningen tillgodoser individens rättigheter.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Framförallt upptäckts av medarbetare själva, i ett antal fall av brukare/klienter/allmänhet som upplyst förvaltningen
Hur många personuppgiftsincidenter har dokumenterats?	21
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	9 anmälda till Integritetsskyddsmyndigheten, 11 informerat berörda personer
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	5

3.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskyddsförordningen (artikel 4.12) ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.”

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag från rapporteringsskyldigheten gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” (se artikel 33). Detta innebär att de flesta personuppgiftsincidenter ska rapporteras till Integritetsskyddsmyndigheten (IMY), inte senare än 72 timmar efter att verksamheten fått vetskap om incidenten.

Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter och friheter, ska rapportering även ske till de berörda registrerade personerna utan dröjsmål.

Dataskyddsförordningen delar alltså in personuppgiftsincidenter i tre kategorier: ingen rapportering, rapportering till IMY samt

rapportering till de berörda personerna. Bristande förmåga att rapportera personuppgiftsincidenter i tid kan leda till sanktioner från IMY:s sida. Alla personuppgiftsincidenter dokumenteras, det vill säga även i de fall då incidenten inte ska rapporteras till IMY där omständigheterna kring personuppgiftsincidenten, dess effekter och vilka korrigerande åtgärder som vidtagits ska framgå. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden och bristande dokumentering är sanktionsgrundande.

3.6.3 Resultat

Förvaltningen har i en knapp majoritet av fallen som anmälts till IMY rapporterat händelserna i tid. Verksamheternas bristande rapportering i tid har i flera fall handlat om att personer som upptäckt incidenten till en början inte varit medvetna om att det just rört sig om en personuppgiftsincident enligt dataskyddsförordningen, varför rapporten kommit först senare.

Det finns förbättringspotential som till stor del bedöms kunna avhjälpas genom att informera om vad en personuppgiftsincident är samt dataskyddsförordningens krav på hanteringen.

3.6.4 DSO anger hur allvarliga bristerna är på en skala

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

Bristerna i att rapportera i tid som i stor utsträckning bedöms bero på kunskapsbrist, anses inte vara så omfattande att de kräver omgående åtgärder. Åtgärder bör dock tas under nästa år och det gäller hela förvaltningen.

3.6.5 DSO ger råd och rekommendationer till PUA

För att avhjälpa bristerna på detta område behöver chefer se till att samtliga medarbetare känner till vad en personuppgiftsincident är och vad medarbetaren ska göra när hen upptäcker den. Detta ämne kan exempelvis vara ett tema på ett APT eller ett inslag under annan lämplig mötesform. Spridning av den lokala rutinen för hantering av

personuppgiftsincidenter är också en viktig del för att förbättra hanteringen.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Registerförteckningen
- Hantering av personuppgifter i incidentrapporeringssystemet IA
- Genomförande av den obligatoriska grundutbildningen i dataskydd

4.2 Syfte

En av dataskyddsombudets viktigaste uppgifter är att övervaka verksamhetens efterlevnad av dataskyddsförordningen. En central del av det arbetet är att göra återkommande granskningar av hur väl dataskyddsförordningen efterlevs. Resultaten av granskningarna påverkar i stor utsträckning vilka beslut verksamheten kan fatta i fråga om dataskyddsåtgärder. För PUA är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under det gångna året och vad resultaten av granskningarna är

4.3 Genomförda granskningar och deras resultat

Registerförteckning

Registerförteckningen är en del av de obligatoriska rapporteringsområdena i denna årsrapport. I årsrapporten från 2022 planerades även detta område som granskningsområde, varför den även ges utrymme i denna del.

Från föregående års bedömning kan konstateras att inga större framsteg gjordes under det gångna året, men att arbetet inleddes under hösten för att återuppta en kontinuerlig uppdatering av registerförteckningen. Bristerna i denna del bedöms på samma sätt som under del 3 denna rapport, där en längre bedömning på detta granskningsområde kan läsas, samt dataskyddsombudets rekommendationer för att avhjälpa bristerna.

	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 av personuppgiftshantering i incidentrapporteringssystemet IA

Ett sätt för dataskyddsombudet att granska förvaltningens regelefterlevnad är att granska personuppgiftshanteringen i olika verksamhetssystem. Staden har en gemensam policy om att inga personuppgifter tillhörande externa personer, exempelvis besökare, förskolebarn eller brukare ska förekomma i incidentrapporteringssystemet IA. Detta bland annat eftersom man bedömt att säkerheten inte kan garanteras för personuppgifterna.

Den 6 november 2023 genomfördes en granskning i IA där 100 händelser kopplade till person i IA mellan datumen 2023-08-09 – 2023-10-27 granskades. Resultatet av granskningen visade att det enbart i 1 av 100 fall förekom personuppgifter, och att det i detta fall var i form av initialer.

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

Genomförande av den obligatoriska grundutbildningen i dataskydd

För att förvaltningen ska kunna leva upp till kraven i dataskyddsförordningen behöver grundläggande kunskaper om dataskydd upprätthållas bland medarbetare och chefer. Staden har

beslutat att alla medarbetare årligen ska genomföra grundutbildning i dataskydd.

Av totalt 213 medarbetare har följande status rapporterats den 11 december 2023:

- 116 har genomfört
- 63 har påbörjat men ej slutfört
- 34 har ej påbörjat

Resultaten visar att ungefär 53 % hade statusen genomfört vid tidpunkten för rapporten. Om man tillägger antalet som hade status påbörjat men ej slutfört uppgår siffran till ca 80 %. Det tillgängliga underlaget talar inte om hur långt de medarbetare kommit som påbörjat utbildningen men ej slutfört. Resterande hade ej påbörjat utbildningen.

Eftersom underlaget inte visar hur långt de medarbetare kommit som hade status påbörjat, går det inte att dra några definitiva slutsatser om antalet vad gäller genomförande eftersom det lika gärna kan vara ett knapptryck som saknas så väl som större delen av utbildningen. Det kan dock konstateras att 80 % av medarbetarna tagit del av delar av utbildningen.

Eftersom utbildningen är obligatorisk är den eftersträvansvärda siffran högre än 80 % för genomförande, och att siffran genomfört vid tillfället enbart var 53 % indikerar att uppföljningen från cheferna har brister. Bristen bedöms dock inte bara omfattande eller kräva omgående åtgärder.

	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

5 Risker inom dataskydd

5.1 Sammanfattning

Ett arbete behöver inledas under 2024 för att kartlägga riskerna inom dataskydd i förvaltningen för att få en mer komplett bild, en kartläggning som görs av dataskyddsombudet. För detta krävs exempelvis en överblick över de system som används och vilka typer av personuppgifter som behandlas, men också att registerförteckningen är uppdaterad och på ett korrekt sätt återger de personuppgiftsbehandlingar som sker.

I nuläget bedöms nedan övergripande rubriker utgöra risker inom dataskyddet:

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

5.2 Syfte

Verksamheten har ansvar för att göra vissa typer av riskanalyser, så som konsekvensbedömningar och informationsklassningar, men dessa ger inte en heltäckande bild av personuppgiftsriskerna i verksamheten. Dataskyddsombudet behöver som underlag för sin egen planering och sitt löpande arbete ha kontinuerlig överblick över dessa risker, i verksamhetens samtliga personuppgiftsbehandlingar.

Exempelvis krävs en sådan överblick för att kunna välja ut vilka områden som bör granskas under det kommande året eller för att avgöra vilka råd som dataskyddsombudet behöver lämna till verksamheten om dataskyddsåtgärder som behöver vidtas.

5.3 Resultatet av riskkartläggningen

Bristande kunskaper i dataskyddsfrågor

Det har under senare år inte genomförts några utbildningar i dataskyddsfrågor på bred front i förvaltningen och under lång tid har lokala stöd- och styrdokument saknats. Bristande kunskaper har också lyfts som en risk i tidigare rapporter. Bristande kunskaper om dataskyddsförordningen och de krav förordningen ställer på personuppgiftshantering innebär en risk av flera skäl. Utan kunskap blir det svårt att upptäcka säkerhetsrisker kring personuppgiftshantering. Det är också svårt att då uppfylla de grundläggande principerna såsom information till registrerade om

hur deras personuppgifter behandlas, principen om lagringsminimering eller principen om ändamålsminimering, att personuppgifter enbart får användas för de syften som de först samlades in för. Bristande kunskaper kan också öka risken för att personuppgiftsincidenter sker, samt att förvaltningen inte på ett korrekt sätt arbetar förebyggande mot risker.

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

Bristerna på området bedöms vara omfattande och kräver omgående åtgärder. Här kommer skillnader finnas mellan enheter och möjligen även avdelningar, men gemensamt är att kunskapslyft på någon nivå behövs i dataskyddsfrågor och att dataskyddsfrågorna integreras på ett sätt som gör att det är lätt att göra rätt och att rätt stöd finns tillgängligt när så behövs.

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

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

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

	Inga brister av nämnvärd betydelse identifierade

Bedömningen är i likhet med de enskilda kategorierna att det utgör allvarliga brister och innebär att förvaltningen idag inte lever upp till kraven som dataskyddsförordningen ställer på hanteringen av känsliga personuppgifter som kan innebära hög risk för registrerades fri- och rättigheter.

5.4 DSO ger råd och rekommendationer till PUA

Gällande kunskapsnivån kan den exempelvis höjas genom att följa upp att samtliga medarbetare årligen fullföljer den obligatoriska grundutbildningen, att sprida den handbok och lokala rutiner som finns och att låta dataskyddsfrågorna ta plats under lämpliga mötesformer. Fortsatt framtagande och spridande av ytterligare lokala rutiner behövs.

Hanteringen av känsliga personuppgifter som kan innebära hög risk för registrerades fri- och rättigheter kan förbättras genom att förvaltningen, utifrån ett riskbaserat arbetssätt, klassar och konsekvensbedömer system och behandlingar där känsliga personuppgifter hanteras i stora mängder så att risker kan förebyggas på det sätt som dataskyddsförordningen kräver.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

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

- *Hantering av personuppgiftsincidenter enligt ny lokal rutin*
- *Granskningar av personuppgiftshantering i verksamhetssystem*
- *Förekomsten av och innehållet i PUB-avtal*
- *Grundläggande principer – särskilt om informationskravet*

6.2 Syfte

Det granskande arbetet är som tidigare nämnt en av dataskyddsombudets viktigaste uppgifter. Eftersom dataskyddsombudet ofta har begränsat med tid, behöver granskningsplanen för det nya året utformas med eftertanke. Som en tumregel bör två-tre granskningar ses som en rimlig granskningsinsats under ett verksamhetsår.

Granskningsområdena bör lämpligen väljas utifrån ett riskbaserat synsätt, det vill säga att fokus bör ligga på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Därigenom åstadkoms en röd tråd i dataskyddsarbetet från ett verksamhetsår till nästa samtidigt som de största riskerna elimineras eller åtminstone sänks till en mer acceptabel nivå.

6.3 Planerade granskningar

Grundläggande principer - Informationskravet

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

Idag saknas en överblick över hur förvaltningen lever upp till detta krav i de olika verksamheterna. En översikt planeras därför att göras under 2024 för att kunna ge rekommendationer om förbättringar på detta område.

Hantering av personuppgiftsincidenter

Särskild uppföljning planeras av hur den nya lokala rutinen för hanteringen av personuppgiftsincidenter efterföljs, och om hanteringen lever upp till kraven som ställs i dataskyddsförordningen. Granskningen kommer ske löpande samt under slutet av året när sammanställningen av årets personuppgiftsincidenter gjorts.

Granskningar i verksamhetssystem

Under 2024 planeras ett antal stickprov genomföras i verksamhetssystem där personuppgifter behandlas. De

verksamhetssystem som kommer att vara aktuella för år 2024 är eDok och Paraplysystemet. Prioriteringen av dessa system utgår från ett riskbaserat arbetssätt då de innehåller stora mängder personuppgifter och till del också känsliga personuppgifter.

I dataskyddsombudets årshjul ligger även att se över förekomsten av och innehållet i PUB-avtal, en översikt som dataskyddsombudet idag saknar.

7 Övrigt att rapportera

Året 2023 har inneburit en omtag kring dataskyddsfrågorna i stadsdelen. Arbete har skett kring framtagande av styrdokument, utvecklande av dataskyddsorganisationen och ett flertal utbildningstillfällen har getts till chefer och dataskyddssamordnare. Ett nätverk mellan dataskyddsombuden i Skarpnäck, Enskede-Årsta-Vantör och Farsta har bildats. Dataskyddsombudet har även tagit fram ett årshjul för det uppföljande arbetet som också publicerats för att öka insyn och förståelse för dataskyddsfrågorna.

Det har av rapporten framkommit att stadsdelen har delvis stora utmaningar i dataskyddsarbetet. Viktiga komponenter vad gäller hanteringen av känsliga personuppgifter saknas och kunskaper om personuppgiftshantering behöver öka brett i organisationen. Utmaningar finns även när det kommer till organisationen för dataskyddsfrågor i staden i stort. Det saknas idag en tydlig centralorganisation för GDPR-frågor i staden, vilket blir synligt i kontakten med andra stadsdelar då stora skillnader finns mellan hur stadsdelar arbetar. En ökad öppenhet, ökad central styrning i delar där det är möjligt och ännu mer samarbete kring exempelvis klassningar och konsekvensbedömningar skulle innebära fördelar i att höja kompetens och öka likvärdighet över staden.

En central faktor för att dataskyddsarbetet i förvaltningens olika delar ska vara framgångsrikt är att det integreras i det dagliga arbetet. Punktinsatser och projekt kan ge kortvariga resultat, men förvaltningen behöver sträva efter kontinuitet, kvalitet och hållbarhet över tid. För att detta ska ske talar erfarenhet för att förvaltningsledningen och övriga chefer har ett avgörande uppdrag i att leda och prioritera arbetet. Förvaltningsledning, chefer, dataskyddsombud och dataskyddssamordnare samt övriga medarbetare har alla –var för sig och tillsammans - viktiga roller i arbetet i att leva upp till dataskyddsförordningens krav och förvalta förtroendet som stockholmarna ger oss.