Stockholms stad

GDPR Årsrapport

År 2023

Enskede-Årsta-Vantörs stadsdelsnämnd

GDPR årsrapport
2023

Dnr: EÅV 2023/996
Utgivningsdatum: 2024-02-22
Kontaktperson: Nicole Melkie

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.

Dataskyddsombudet bedömer att stadsdelsnämnden överlag har bra ordning och rutiner för dataskyddsarbetet och att stadsdelsnämnden följer gällande lagstiftning.

Dataskyddsombudet har identifierat vissa brister i dataskyddsarbetet och utifrån detta lämnat en del råd och rekommendationer till stadsdelsnämnden. Brister har identifierats inom områdenakonsekvensbedömning och uppföljning av personuppgiftsbiträdesavtal. De brister som identifierats bedöms dock inte vara omfattande, brådskande eller av allvarlig karaktär.

3 Obligatoriska rapporteringsområden

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

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

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

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	582.
Har nödvändiga uppdateringar gjorts?	Ja, till största del.
Bedöms registerförteckningen vara fullständig?	Ja, till största del.
Har verksamheten lämpliga rutiner för registerföring?	Ja.

3.1.2 Syfte

Enligt artikel 30 i dataskyddsförordningen är stadsdelsnämnden skyldig att inventera alla personuppgifter som behandlas i verksamheten och dokumentera personuppgiftsbehandlingarna i en så kallad registerförteckning.

Registerförteckningen är dataskyddsarbetets centrala utgångspunkt och bas. Registerförteckningen säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling. Registerförteckningen möjliggör dessutom att verksamheten kan arbeta effektivt, systematiskt och riskbaserat med dataskyddsfrågor, samtidigt som individens integritet värnas.

Syftet med detta rapporteringsområde är att rapportera till stadsdelsnämnden hur väl verksamheten har lyckats inventera sina personuppgifter samt upprätta en aktuell och fullständig registerförteckning.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats
Enskede-Årsta-Vantörs stadsdelsnämnd använder det digitala verktyget Draftit för att registerföra personuppgiftsbehandlingar.

Den 28 november 2023 hade stadsdelsnämnden totalt 582 personuppgiftsbehandlingar i registerförteckningen i Draftit.

- *184 av dessa hade status Godkänd*
- *45 av dessa hade status Under bearbetning*
- *320 av dessa hade status Redo för granskning*
- *33 av dessa hade status Komplettering begärd*
- *0 av dessa hade status Under granskning*

DSO kontrollerar om nödvändiga uppdateringar gjorts

Enligt förvaltningens rutin för inventering av personuppgiftsbehandlingar ska översyn av registerförteckningen ske under kvartal 1. I slutet av april 2023 följde dataskyddsombudet upp att alla avdelningar hade inventerat sina personuppgiftsbehandlingar och gjort nödvändiga uppdateringar i Draftit. Uppföljningen skedde genom att frågor ställdes till alla avdelningschefer och dataskyddssamordnare via mejl.

Följande frågor ställdes till avdelningschefer och dataskyddssamordnare:

1. Har avdelningens registreringar i Draftit setts över under året och vid behov uppdaterats?
    a. Har din avdelning kontrollerat att man har rätt formulär (mallar) i sina registreringar?

2. Om svaret är nej på första frågan – varför har det inte skett? Finns det någon plan för när det kommer att ske?

Uppföljningen visade följande:

- Avdelning HR och utveckling, Social omsorg äldre, Social omsorg vuxen, Social omsorg barn och unga och Social omsorg förebyggande och främjande hade sett över och vid behov uppdaterat sina registreringar.
- Administrativa avdelningen och Avdelning förskola hade till största del sett över och vid behov uppdaterat sina registreringar.

Dataskyddsombudet samlade bedömning är att nödvändiga uppdateringar till största del har gjorts.

DSO bedömer hur fullständig registerförteckningen är

Eftersom dataskyddsombudet uppskattar att nödvändiga uppdateringar till största del har skett i registerförteckningen så är dataskyddsombudet samlade bedömning att registerförteckningen till största del är fullständig och aktuell.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Dataskyddsombudet bedömer att förvaltningen har lämpliga rutiner för registerföring. Förvaltningen har sedan januari 2021 en rutin för inventering av personuppgiftsbehandlingar. Enligt rutinen ansvarar varje avdelningschef för att inventering av behandlingar sker på avdelningen. Inventeringen ska genomföras årligen under kvartal ett och nödvändiga uppdateringar ska göras i Draftit utifrån inventeringen.

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

Dataskyddsombudet har inte identifierat några nämnvärda brister. Förvaltningen har sedan januari 2021 en rutin för inventering av personuppgiftsbehandlingar. Rutinen för inventering av personuppgiftsbehandlingar har uppdaterats under maj 2023. Dataskyddsombudet bedömer att förankringen av rutinen är bättre än föregående år då dataskyddsombudet upplever att verksamheterna har bättre kännedom om rutinen samt att fler personuppgiftsbehandlingar har registrerats i Draftit.

3.1.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet har inte identifierat några nämnvärda brister och har därför inga särskilda råd eller rekommendationer till stadsdelsnämnden när det gäller registerförteckningen.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Till största del.
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Ja, förutom rutinen för hantering av personuppgiftsincidenter.
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Ja, förutom rutinen för hantering av personuppgiftsincidenter.
Är dokumenten uppdaterade?	Ja, till största del.
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja

3.2.2 Syfte

En röd tråd i dataskyddsförordningen är att viktiga arbetssätt och rutiner ska vara dokumenterade. Detta följer bland annat av artikel 5 i dataskyddsförordningen där det framgår att stadsdelsnämnden ska kunna visa att dataskyddsförordningens principer för behandling av personuppgifter efterlevs.

Syftet med detta rapporteringsområde är att bedöma om stadsdelsnämnden har relevanta styrdokument på plats samt att styrdokumenten håller en lämplig kvalitet.

Genom styrdokument kan stadsdelsnämnden visa att den bedriver ett systematiskt dataskyddsarbete och att den styr hur anställda ska behandla personuppgifter. Att styrdokument finns nedtecknade och att de är beslutade och kommunicerade medför att anställda får information om dataskydd samt kan behålla kunskapen över tid och tillämpa den på ett konsekvent sätt.

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?
Dataskyddsombudet har den 16 maj 2023 sökt på intranätet efter vilka rutiner och andra styrdokument förvaltningen har kring

dataskydd. På förvaltningens sida om dataskydd finns följande rutiner och styrdokument:

- Handbok för behandling av personuppgifter
- Rutin för inventering av personuppgiftsbehandlingar
- Rutin för hantering av personuppgiftsincidenter
- Rutin för konsekvensbedömning
- Rutin för personuppgiftsbiträdesavtal
- Rutin för hantering av registrerades rättigheter
- Anvisningar för hantering av personuppgifter för Avdelning förskola

I årsrapporten för 2022 konstaterade dataskyddsombudet att förvaltningens styrdokument skrevs under 2021 och skulle därför behöva ses över och vid behov uppdateras. Informationssäkerhetssamordnaren, i samråd med dataskyddsombudet, har under våren 2023 sett över och uppdaterat flertal av styrdokument där det funnits behov.

I årsrapporten för 2022 konstaterade dataskyddsombudet att förvaltningen saknade en dokumentägare för handboken för behandling av personuppgifter. Informationssäkerhetssamordnaren, i samråd med dataskyddsombudet, har under våren 2023 uppdaterat dokumentägare.

Förvaltningen har sedan sommaren 2023 uppdaterade styrdokument på intranätet.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

I årsrapporten från 2021 bedömde dataskyddsombudet att rutinen för hantering av personuppgiftsincidenter inte håller lämplig kvalitet. Informationssäkerhetssamordnaren fick därför i uppdrag att under 2022 ta fram en skriftlig rutin för hantering av personuppgiftsincidenter. Eftersom rutinen inte togs fram under 2022 kvarstod rekommendationen under 2023. Vid kontroll i slutet av år 2023 har en ny rutin för hantering av personuppgiftsincidenter ännu inte färdigställts. Därför kvarstår denna rekommendation. Det framgår i rutinen att personuppgifter ska dokumenteras men inte hur (exempelvis om de ska diarieföras eller inte). Rutinen anger inte tydligt hur en personuppgiftsincident ska utredas och när den ska rapporteras till Integritetsskyddsmyndigheten.

Enligt rutinen är det dataskyddsombudet som, i samråd med ansvarig chef, ska ta ställning till om en personuppgiftsincident ska rapporteras till Integritetsskyddsmyndigheten eller inte. Detta

stämmer varken överens med dataskyddsombudets roll (dataskyddsombudet ska vara rådgivande och reviderande – inte beslutsfattande) eller med stadsdelsnämndens delegationsordning (enligt delegationsordningen är det enhetschef som avgör om en personuppgiftsincident ska rapporteras till tillsynsmyndigheten).

Vidare står det ingenting om när och hur registrerade ska få information om inträffade personuppgiftsincidenter. Det står heller inget om informationssäkerhetssamordnarens roll vid personuppgiftsincidenter, till exempel att informationssäkerhetssamordnaren ska informera stadens informationssäkerhetsansvarig om personuppgiftsincidenter som har anmälts till Integritetsskyddsmyndigheten.

I övrigt bedömer dataskyddsombudet att de skriftliga dokument som finns på förvaltningen håller en lämplig kvalitet.

3.2.4 DSO anger hur allvarliga bristerna är på en skala

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

Dataskyddsombudet har identifierat brister som bör åtgärdas. Bristerna bedöms dock inte vara omfattande eller allvarliga. Brister har identifierats i förvaltningens rutin för hantering av personuppgiftsincidenter.

3.2.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet rekommenderar att stadsdelsnämnden ger informationssäkerhetssamordnaren i uppdrag att, i samråd med dataskyddsombudet, uppdatera rutinen för hantering av personuppgiftsincidenter. I rutinen bör följande tydliggöras:

- Hur personuppgiftsincidenter ska utredas
- När en personuppgiftsincident ska rapporteras till tillsynsmyndigheten
- När och hur registrerade ska få information vid personuppgiftsincidenter
- Hur personuppgiftsincidenter ska dokumenteras

- Ansvarsfördelning mellan chef, informationssäkerhetssamordnare och dataskyddsombud

Vidare föreslår dataskyddsombudet att stadsdelsnämnden ger dataskyddsombudet i uppdrag att följa upp att detta har genomförts och att rapportera resultatet i årsrapporten för 2024 till nämnden.

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?	57 stycken.
Är klassade personuppgiftsbehandlingar aktuella?	Ja.

3.3.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd ska verksamheten informationsklassa sin information. Enligt Stockholms stads riktlinjer för informationssäkerhet ska alla stadens informationstillgångar vara klassade med stöd av verktyget KLASSA. Utan informationsklassningen har verksamheten inte förutsättningar att välja rätt åtgärder för att skydda sin information.

Syftet med detta rapporteringsområde är att rapportera till stadsdelsnämnden om informationsklassning är genomförd för de personuppgifter som verksamheten behandlar.

3.3.3 Resultat

Förvaltningen har en förteckning över informationsklassning som administreras av informationssäkerhetssamordnaren. Där framgår det bland annat vilka informationstillgångar som har informationsklassats och när. Den 31 augusti 2023 har dataskyddsombudet granskat förteckningen.

Förteckningen visar följande:

- Det finns 113 stycken informationstillgångar som innehåller personuppgifter och omfattas av dataskyddsförordningen.
    - 57 stycken av dessa har informationsklassats.

Detta kan jämföras med år 2022 då 103 informationstillgångar innehöll personuppgifter och 22 av dessa hade informationsklassats.

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

Dataskyddsombudet bedömer att det inte finns några brister av nämnvärd betydelse. Detta eftersom informationssäkerhetssamordnaren har upprättat en prioritetsordning för informationsklassningarna och fortsatt arbetet enligt dataskyddsombudets rekommendation i 2021 års årsrapport.

3.3.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet har inte identifierat några nämnvärda brister och har därför inga särskilda råd eller rekommendationer till stadsdelsnämnden när det gäller tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Ja.
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Nej. Social omsorg barn och unga och Social omsorg förebyggande och främjande behöver genomföra konsekvensbedömningar.
Är de genomförda bedömningarna aktuella?	Delvis.

3.4.2 Syfte

Personuppgiftsbehandlingar som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska konsekvensbedömas enligt artikel 35.1 i dataskyddsförordningen. Syftet med en konsekvensbedömning är att identifiera och dokumentera risker kopplade till en viss personuppgiftsbehandling samt att bedöma sannolikheten och konsekvensen om riskscenariot skulle inträffa. Utifrån bedömningen ska eventuella riskförebyggande åtgärder vidtas.

Konsekvensbedömning är ett viktigt verktyg för verksamhetens dataskyddsarbete. Den hjälper verksamheten att identifiera och minimera integritetsrisker för personuppgifter som behandlas i verksamheten.

Syftet med detta rapporteringsområde är att rapportera till stadsdelsnämnden om alla personuppgiftsbehandlingar som borde konsekvensbedömas har identifierats och konsekvensbedömts.

3.4.3 Resultat

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

Förvaltningen använder systemet Draftit som stöd för att genomföra konsekvensbedömningar. Den 28 juni 2023 har dataskyddsombudet kontrollerat i systemet vilka avdelningar som har genomfört

konsekvensbedömningar. Samtliga avdelningar har genomfört flera konsekvensbedömningar i systemet. Samtliga avdelningar har behandlingar som skulle kunna leda till hög risk och därmed behöver konsekvensbedömas.

Eftersom information har gått ut i dataskyddsnätverket och flera konsekvensbedömningar har genomförts av berörda avdelningar bedömer dataskyddsombudet att förvaltningen har identifierat de personuppgiftsbehandlingar som behöver konsekvensbedömas. Alla konsekvensbedömningar har dock ännu inte genomförts. Se mer information nedan.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?
Dataskyddsombudet konstaterade i årsrapporten för 2021 att konsekvensbedömning ännu inte genomförts för alla potentiella högriskbehandlingar. Denna bedömning återstår.

Social omsorg barn och unga och Social omsorg förebyggande och främjande behöver genomföra konsekvensbedömningar för enheter inom avdelningarna.

Är de genomförda konsekvensbedömningarna aktuella?
Dataskyddsombudet har den 28 juni 2023 granskat i Draftit vid vilken tidpunkt avdelningarna har genomfört konsekvensbedömningar. För samtliga avdelningar var det länge sedan vissa konsekvensbedömningar genomfördes. Avdelningarna genomförde vissa av sina konsekvensbedömningar mellan 2019-2022.

3.4.4 DSO anger hur allvarliga bristerna är på en skala

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

Dataskyddsombudet bedömer att det finns brister i arbetet med konsekvensbedömning som bör åtgärdas. Bristerna är dock inte omfattande eller allvarliga. Bedömningen grundar sig på att Social omsorg barn och unga och Social omsorg förebyggande och främjande inte har konsekvensbedömt alla högriskbehandlingar.

3.4.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet rekommenderar att stadsdelsnämnden ger avdelningschefer för Social omsorg barn och unga och Social omsorg förebyggande och främjande i uppdrag att konsekvensbedöma högriskbehandlingar under 2024. Dataskyddsombudet rekommenderar även stadsdelsnämnden att ge samtliga avdelningschefer i uppdrag att se över om konsekvensbedömningar behöver uppdateras om under 2024.

Vidare föreslår dataskyddsombudet att stadsdelsnämnden ger dataskyddsombudet i uppdrag att följa upp att detta har genomförts och att rapportera resultatet i årsrapporten för 2024 till nämnden.

3.5 Individens rättigheter

3.5.1 Sammanfattning

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

3.5.2 Syfte

Registrerade personer har enligt artikel 12-22 i dataskyddsförordningen ett antal rättigheter. Rättigheterna ska på olika sätt garantera att den registrerade har insyn i hur dennes personuppgifter hanteras och har en viss kontroll över personuppgiftsbehandlingen.

Rättigheterna innebär att registrerade kan begära följande:

- Ett registerutdrag där det framgår vilka personuppgifter förvaltningen behandlar om personen och hur förvaltningen behandlar uppgifterna
- Rättelse av felaktiga personuppgifter
- Radering av personuppgifter
- Begränsning av en behandling av personuppgifter
- Hjälp med att flytta personuppgifter (dataportabilitet)
- Invända mot en behandling av personuppgifter

Begäran ska utredas och besvaras inom en månad från att den inkom. Vid behov får tiden förlängas med ytterligare två månader. Hänsyn ska tas till hur komplicerad begäran är och antalet inkomna begäranden. Den sökande ska informeras om förlängningen och anledningen till detta.

Syftet med detta rapporteringsområde är att rapportera stadsdelsnämnden hur väl 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?
Dataskyddsombudet bedömer att förvaltningen har förutsättningar för att hantera registrerades rättigheter inom föreskriven tid.

Förvaltningen har en rutin för hur registrerades rättigheter ska hanteras. Dataskyddsombudet för ett register över begäran som har inkommit.

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

Dataskyddsombudet har inte identifierat några nämnvärda brister.

3.5.5 DSO ger råd och rekommendationer till PUA
Dataskyddsombudet har inte identifierat några nämnvärda brister och har därför inga särskilda råd eller rekommendationer till stadsdelsnämnden när det gäller hantering av registrerades rättigheter.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Vanligtvis genom information från anställd eller utomstående.
Hur många personuppgiftsincidenter har dokumenterats?	Totalt 33 stycken.
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	15 incidenter har rapporterats till Integritetsskyddsmyndigheten. 8 incidenter har informerats till berörda personer.
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Fem incidenter har inte rapporterats in i tid till Integritetsskyddsmyndigheten.

3.6.2 Syfte

Enligt artikel 4.12 i dataskyddsförordningen är en personuppgiftsincident ”*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*.”

Personuppgiftsincidenter ska som huvudregel rapporteras till Integritetsskyddsmyndigheten, om det inte är osannolikt att personuppgiftsincidenten medför en risk för registrerade personers rättigheter och friheter enligt artikel 33 i dataskyddsförordningen. Rapportering till Integritetsskyddsmyndigheten ska ske inom 72 timmar från det att verksamheten får vetskap om incidenten. Om personuppgiftsincidenten sannolikt leder till hög risk för registrerade personers rättigheter och friheter ska personerna informeras om incidenten.

Alla personuppgiftsincidenter ska dokumenteras enligt artikel 33.5 i dataskyddsförordningen, oavsett om de rapporteras till tillsynsmyndigheten eller inte.

Syftet med detta rapporteringsområde är att redogöra för stadsdelsnämnden om verksamheten har förmåga att rapportera personuppgiftsincidenter i tid samt vilka typer av personuppgiftsincidenter som har inträffat i verksamheten under året.

3.6.3 Resultat

Hur väl förmår verksamheten att rapportera personuppgiftsincidenter i tid till Integritetsskyddsmyndigheten?
Personuppgiftsincidenter upptäcks vanligtvis genom att anställda eller utomstående informerar om att det har inträffat en incident.

Enligt förvaltningens rutin ska alla personuppgiftsincidenter som sker i förvaltningen rapporteras till dataskyddsombudet. Detta sker genom att verksamheten fyller i en blankett och mejlar den till dataskyddsombudet. Verksamheten ska även dokumentera incidenten i IA. Dataskyddsombudet bedömer att verksamheterna är bra på att rapportera personuppgiftsincidenter till dataskyddsombudet.

Dataskyddsombudet har en lista över alla inträffade personuppgiftsincidenter i förvaltningen. Den 28 november 2023 hade totalt 33 personuppgiftsincidenter inträffat under 2023. 15 av dessa har rapporterats vidare till Integritetsskyddsmyndigheten och rapportering har skett i tid i alla utom fem fall. Incidenterna som inte rapporterades i tid har varit incidenter som dataskyddsombudet inte fått skickat till sig inom 72 timmar från att incidenterna upptäcktes. En av dessa incidenter har berört annan förvaltning.. Enhetschef väntade då på att få mer information från den andra förvaltningen innan incidenten rapporterades till dataskyddsombudet. De andra fyra incidenterna visar på brister i organisatoriska rutiner då medarbetare inte kände till att de behövde rapportera in incidenterna till dataskyddsombudet. I endast åtta fall har de registrerade fått information om inträffade incidenter. Registrerade bör få information i alla inträffade incidenter.

De flesta personuppgiftsincidenter som inträffat i förvaltningen handlar om att uppgifter har skickats till fel mottagare samt borttappade dokument.

I årsrapporten 2021 identifierade dataskyddsombudet att verksamheterna inte riktigt vet vad de ska göra vid förlust av dator eller telefon. Informationssäkerhetssamordnaren fick 2022 i

uppdrag att ta fram en skriftlig rutin för vad som ska göras vid förlust av arbetstelefon eller arbetsdator. Vid en kontroll av dataskyddsombudet den 10 oktober 2023 har en sådan påbörjats av Informationssäkerhetssamordnaren.

Som nämnt i kapitel 3.2 Styrdokument bedömde dataskyddsombudet i årsrapporten från 2021 att rutinen för hantering av personuppgiftsincidenter inte håller lämplig kvalitet. Informationssäkerhetssamordnaren fick därför i uppdrag att under 2022 ta fram en skriftlig rutin för hantering av personuppgiftsincidenter. Eftersom rutinen inte togs fram under 2022 kvarstod rekommendationen under 2023. Vid kontroll i slutet av år 2023 har en ny rutin för hantering av personuppgiftsincidenter ännu inte färdigställts. Därför kvarstår denna rekommendation.

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

Dataskyddsombudet har identifierat brister som bör åtgärdas. Bristerna är dock inte omfattande eller allvarliga. Bedömningen grundar sig på att förvaltningen inte har en färdigställd skriftlig rutin för vad som ska göras i samband med förlust av arbetstelefon eller arbetsdator. Bedömningen grundar sig även på att rutinen för hantering av personuppgiftsincidenter inte heller är färdigställd.

3.6.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet rekommenderar att stadsdelsnämnden ger informationssäkerhetssamordnaren i uppdrag att färdigställa en skriftlig rutin för vad som ska göras vid förlust av arbetstelefon eller arbetsdator, samt att färdigställa en skriftlig rutin för hantering av personuppgiftsincidenter.

Vidare föreslår dataskyddsombudet att stadsdelsnämnden ger dataskyddsombudet i uppdrag att följa upp att detta har genomförts och att rapportera resultatet i årsrapporten för 2024 till nämnden.

4 Övrigt att rapportera

4.1 Sammanfattning

4.2 Uppföljning av personuppgiftsbiträdesavtal

4.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns rutin för uppföljning av personuppgiftsbiträdesavtal?	Nej.
Har uppföljning av personuppgiftsbiträdesavtal under 2023 skett?	Ja.

4.2.2 Syfte

Den som behandlar personuppgifter för en personuppgiftsansvarigs räkning är ett personuppgiftsbiträde. I dessa fall ska, enligt artikel 28 i dataskyddsförordningen, ett personuppgiftsbiträdesavtal tecknas mellan den personuppgiftsansvarige och personuppgiftsbiträdet.

I 2022 års granskningsrapport fick dataskyddsombudet i uppdrag att, utöver de sex obligatoriska områdena som granskats ovan, granska verksamhetens uppföljning av personuppgiftsbiträdesavtal.

Syftet med detta rapporteringsområde är att rapportera till stadsdelsnämnden om verksamheten har styrdokument för uppföljning av personuppgiftsbiträdesavtal och i vilken omfattning uppföljningen sker i praktiken.

4.2.3 Resultat

Dataskyddsombudet har den 27 november 2023 sökt på intranätet efter vilka rutiner och andra styrdokument förvaltningen har kring uppföljning av personuppgiftsbiträdesavtal. Förvaltningen har en rutin för personuppgiftsbiträdesavtal, vilket nämns i avsnitt 3.2. Förvaltningen har dock inte någon skriftlig rutin för uppföljning av personuppgiftsbiträdesavtal.

Dataskyddsombudet har en lista på förvaltningens aktuella personuppgiftsbiträdesavtal. Denna lista har genom mejl stämts av med berörda dataskyddssamordnare. Dataskyddsombudet har frågat om avdelningarnas personuppgiftsbiträdesavtal är aktuella och om någon uppföljning av dessa har skett under 2023.

Samtliga avdelningar har genomfört uppföljning på sina personuppgiftsbiträdesavtal en gång under 2023.

4.2.4 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

Dataskyddsombudet bedömer att det finns brister i arbetet med uppföljning av personuppgiftsbiträdesavtal som bör åtgärdas. Bristerna är dock inte omfattande eller allvarliga. Bedömningen grundar sig på att förvaltningen inte har något styrdokument för uppföljning av personuppgiftsbiträdesavtal.

4.2.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet rekommenderar att stadsdelsnämnden ger avdelningschef för Administrativa avdelningen, i samråd med dataskyddsombudet, i uppdrag att ta fram en skriftlig rutin för uppföljning av personuppgiftsbiträdesavtal.

Vidare föreslår dataskyddsombudet att stadsdelsnämnden ger dataskyddsombudet i uppdrag att följa upp att detta har genomförts och att rapportera resultatet i årsrapporten för 2024 till nämnden.

5 Planerade granskningar under det nya verksamhetsåret

5.1 Sammanfattning

Under 2024 kommer dataskyddsombudet att genomföra granskningar utifrån de obligatoriska rapporteringsområdena. Dataskyddsombudet kommer även att följa upp att de brister som dataskyddsombudet har identifierat i denna årsrapport har åtgärdats.

5.2 Syfte

En av dataskyddsombudets viktigaste uppgifter är det granskande arbetet. Granskningsområdena styrs dels av de obligatoriska rapporteringsområdena (registerförteckning, styrdokument, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, konsekvensbedömningar, individens rättigheter och personuppgiftsincidenter). Utöver det kan dataskyddsombudet välja ut ytterligare områden som ska granskas. Urvalet sker utifrån ett riskbaserat synsätt.

5.3 Planerade granskningar

5.3.1 Obligatoriska rapporteringsområdena

Dataskyddsombudet kommer att genomföra granskningar utifrån de obligatoriska rapporteringsområdena:

- Registerförteckning
- Styrdokument
- Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar
- Konsekvensbedömningar
- Individens rättigheter
- Personuppgiftsincidenter

Dataskyddsombudet kommer även att följa upp om åtgärder har vidtagits inom dessa områden utifrån de rekommendationer dataskyddsombudet har lämnat i denna årsrapport för 2023.