Stockholms stad

Dataskyddsombudets årsrapport GDPR

2021

Enskede-Årsta-Vantörs stadsdelsnämnd

Dataskyddsombudets årsrapport GDPR 2021

Dnr: EÅV 2021/1011
Utgivningsdatum: 2022-02-24
Kontaktperson: Emma Ekelund

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. 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”). Dataskyddsombudet har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är ett medel för Enskede-Årsta-Vantörs stadsdelsnämnd att ta emot de råd och rekommendationer som dataskyddsombudet är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad dataskyddsombudets granskande arbete visar. Årsrapporten syftar till att stadsdelsnämnden ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för stadsdelsnämnden att visa hur stadsdelsnämnden i egenskap av personuppgiftsansvarig (”PUA”) efterlever dataskyddsförordningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att stadsdelsnämnden ska kunna visa att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna dokumenteringsskyldighet. Årsrapporten är även ett medel för stadsdelsnämndens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehåll

2 Sammanfattning

I egenskap av dataskyddsombud lämnar jag följande årsrapport.

Dataskyddsombudets bedömer att stadsdelsnämnden överlag har bra koll på 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 följande områden: styrdokument, tekniska och organisatoriska säkerhetsåtgärder för personuppgiftsbehandlingar, konsekvensbedömning och personuppgiftsincidenter. De flesta brister bedöms dock inte vara omfattande, brådskande eller av allvarlig karaktär.

Den mest utmärkande och omfattande bristen som dataskyddsombudet har identifierat är arbetet med informationsklassning. Vid en kontroll den 12 november 2021 hade bara 3 av 60 informationstillgångar som innehåller personuppgiftsincidenter informationsklassats. Dataskyddsombudet rekommenderar därför stadsdelsnämnden att ge informationssäkerhetssamordnaren i uppdrag att, i samråd med avdelningarna, upprätta en plan för när informationsklassning ska ske av olika informationstillgångar och påbörja arbetet med informationsklassning enligt plan.

3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som stadsdelsnämnden 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
- Personuppgiftsincidenter

I denna rapport redogörs för stadsdelsnämndens status och dataskyddsombudets slutsatser samt rekommendationer gällande de uppföljningar och granskningar som dataskyddsombudet har genomfört.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	533.
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 5 november 2021 hade stadsdelsnämnden totalt 533 personuppgiftsbehandlingar i registerförteckningen i Draftit.

- 460 av dessa hade status *Godkänd*
- 32 av dessa hade status *Under bearbetning*
- 13 av dessa hade status *Redo för granskning*
- 27 av dessa hade status *Komplettering begärd*
- 1 av dessa hade status *Under granskning*

DSO kontrollerar om nödvändiga uppdateringar gjorts

I april 2021 följde dataskyddsombudet upp att alla avdelningar hade inventerat sina personuppgiftsbehandlingar och gjort nödvändiga uppdateringar i Draftit i enlighet med förvaltningens rutin för inventering av personuppgiftsbehandlingar. Uppföljningen skedde genom att kontrollfrågor ställdes till alla avdelningschefer via mejl.

Följande frågor ställdes till respektive avdelningschef:

1. Har avdelningens registreringar i Draftit setts över under året och vid behov uppdaterats?
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 Stadsmiljö och lokaler, HR-avdelningen, avdelning Social omsorg vuxen och avdelning Social omsorg äldre hade sett över och vid behov uppdaterat sina registreringar.
- Administrativa avdelningen och avdelning Förskola hade delvis sett över och vid behov uppdaterat sina registreringar.
- Avdelning Social omsorg barn och unga hade inte hunnit se över sina registreringar, men har planerat att göra en större översyn framöver. Dataskyddsombudet har den 26 november 2021 haft ett möte med dataskyddssamordnarna på avdelning Social omsorg barn och unga. De informerade då att avdelningen håller på att se över 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

Förvaltningen har sedan januari 2021 en rutin för inventering av personuppgiftsbehandlingar. Enligt dataskyddsombudets bedömning hade rutinen inte helt förankrats i förvaltningen i början av 2021. Dataskyddsombudet har under hösten påmint avdelningschefer och avdelningarnas dataskyddssamordnare om att inventering ska ske under kvartal ett år 2022 och att dataskyddsombudet kommer att följa upp detta i april 2022. Dataskyddsombudet kommer fortsätta att regelbundet påminna avdelningarna om rutinen. Dataskyddsombudet bedömer därför att de brister som har identifierats kommer att åtgärdas i takt med att rutinen förankras i förvaltningen.

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. Det saknas skriftlig rutin för publicering av nämndhandlingar på webben.
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.
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Handboken för behandling av personuppgifter saknar en dokumentägare.

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 7 november 2021 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

Alla dokument är nyligen uppdaterade. Alla dokument förutom handboken för behandling av personuppgifter har en dokumentägare.

Rutin för hur förvaltningen hanterar information till den registrerade enligt artikel 12, 13 och 14 i dataskyddsförordningen finns i förvaltningens handbok för behandling av personuppgifter. Förvaltningen har även skriftliga standardtexter som kan användas när verksamheterna ska informera de registrerade.

Förvaltningen saknar en skriftlig rutin för publicering av nämndhandlingar som innehåller personuppgifter på webben. Enligt nämndsekreteraren finns det en skriftlig användarmanual för publicering av nämndhandlingar på webben. Om denna manual skulle följas skulle dock inte allmänheten kunna ta del av medborgarförslag. Nämndsekreteraren gör därför en kopia av medborgarförslag och maskar förslagsställarnas personuppgifter innan publicering på webben. Förtroendevaldas och tjänstepersoners personuppgifter är offentliga. Sekretessärenden publiceras aldrig på webben.

Publicering av övriga handlingar och personuppgifter på webben görs av stadsledningskontoret. Stadsledningskontoret har en skriftlig rutin för detta.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

Dataskyddsombudet bedömer att rutinen för hantering av personuppgiftsincidenter inte håller lämplig kvalitet. 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 tillsynsmyndigheten.

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. Förvaltningen saknar dessutom en skriftlig rutin för publicering av nämndhandlingar som innehåller personuppgifter på webben.

3.2.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet rekommenderar att stadsdelsnämnden ger nämndsekreteraren i uppdrag att, i samråd med dataskyddsombudet, ta fram en skriftlig rutin för publicering av nämndhandlingar som innehåller personuppgifter på webben.

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

Dataskyddsombudet rekommenderar dessutom att stadsdelsnämnden ger informationssäkerhetssamordnaren i uppdrag att, i samråd med dataskyddsombudet, tydliggöra vem som ska vara dokumentägare för handboken för behandling av personuppgifter.

Vidare föreslår dataskyddsombudet att stadsdelsnämnden ger dataskyddsombudet i uppdrag att följa upp att detta har genomförts och att rapportera resultatet i årsrapporten för 2022 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?	Tre.
Är klassade personuppgiftsbehandlingar aktuella?	Delvis. Två är aktuella och en inaktuell.

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

Dataskyddsombudet har den 12 november 2021 kontrollerat i Draftit vilka personuppgiftsbehandlingar som har informationsklassats. I Draftit finns två mallar för registrering; en gammal version och en ny version. I den gamla versionen finns det ingen fråga om informationsklassning. I den nya versionen finns det en fråga om informationsklassning. Nästan alla behandlingar är registrerade i den gamla versionen. Draftit ger därför inte en rättvisande bild över vilka behandlingar som har informationsklassats.

Förvaltningen har en förteckning över informationsklassning som administreras av informationssäkerhetssamordnaren. Där framgår det bland annat vilka informationstillgångar som innehåller personuppgifter, om informationstillgångarna har informationsklassats och när. Den 12 november 2021 har dataskyddsombudet granskat förteckningen.

Förteckningen visar följande:

- Det finns 60 stycken informationstillgångar som innehåller personuppgifter och omfattas av dataskyddsförordningen.
- Tre av dessa har informationsklassats:
    - Integra Cloud 2017 (genomförd innan 2018 och anses därmed vara inaktuell)
    - Mina meddelanden 2021 (aktuell)
    - Vodok 2021 (aktuell)

3.3.4 DSO anger hur allvarliga bristerna är på en skala

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

Eftersom endast 3 av 60 informationstillgångar som innehåller personuppgifter har informationsklassats, varav en informationsklassning är inaktuell, bedömer dataskyddsombudet att bristerna är omfattande.

3.3.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet rekommenderar att stadsdelsnämnden ger informationssäkerhetssamordnaren i uppdrag att, i samråd med avdelningarna, upprätta en plan för när informationsklassning ska ske av olika informationstillgångar och påbörja arbetet med informationsklassning enligt plan.

Vidare föreslår dataskyddsombudet att stadsdelsnämnden ger dataskyddsombudet i uppdrag att följa upp att detta har genomförts och att rapportera resultatet i årsrapporten för 2022 till nämnden.

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. Avdelning Social omsorg barn och unga och Administrativa avdelningen behöver genomföra konsekvensbedömningar.
Är de genomförda bedömningarna aktuella?	Delvis. Avdelning Förskola behöver se över genomförda konsekvensbedömningar och planerar att påbörja detta i januari 2021.

3.4.2 Syfte

Personuppgiftsbehandlingar som sannolikt leder till en hög risk för fysiska personer 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 med 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?
Avdelningarnas dataskyddssamordnare har på förvaltningens dataskyddsnätverk den 9 november 2018, 13 februari 2019, 29 maj 2019 och 3 december 2019 fått information om att personuppgiftsbehandlingar som ska konsekvensbedömas behöver identifieras av respektive avdelning.

Förvaltningen använder systemet Draftit som stöd för att genomföra konsekvensbedömningar. Den 11 november 2021 har dataskyddsombudet kontrollerat i systemet vilka avdelningar som har genomfört konsekvensbedömningar. HR-avdelningen, avdelning Förskola, avdelning Social omsorg barn och unga, avdelning Social omsorg vuxen och avdelning Social omsorg äldre har genomfört flera konsekvensbedömningar i systemet. Dessa avdelningar är de avdelningar inom förvaltningen som främst har behandlingar som skulle kunna leda till hög risk och därmed behöver konsekvensbedömas. Detta utifrån att dessa avdelningar hanterar känsliga personuppgifter och uppgifter som omfattas av sekretess om sårbara personer (förskolebarn, anställda och klienter inom socialtjänst).

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 nedan.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?
Enligt dataskyddsombudets bedömningar har konsekvensbedömning ännu inte genomförts för alla potentiella högriskbehandlingar.

Inom avdelning Social omsorg barn och unga har konsekvensbedömningar bara genomförts för personuppgiftsbehandlingar som sker inom enheten för utveckling och främjande arbete. Avdelning Social omsorg barn och unga behöver även genomföra konsekvensbedömningar för övriga enheter inom avdelningen.

Vidare behöver Administrativa avdelningen genomföra konsekvensbedömningar kopplade till sociala delegationen och arkivet.

Är de genomförda konsekvensbedömningarna aktuella?
Dataskyddsombudet har den 12 november 2021 granskat i Draftit vid vilken tidpunkt avdelningarna har genomfört konsekvensbedömningar. För några avdelningar och enheter var det länge sedan konsekvensbedömningar genomfördes. Det gäller avdelning Förskola, HR-avdelningen och beställarenheten funktionsnedsättning och socialpsykiatri inom avdelning Social omsorg vuxen. Dessa avdelningar och enheter genomförde sina konsekvensbedömningar i slutet av 2019 och början av 2020.

Dataskyddsombudet har mejlat berörda avdelningars och enheters dataskyddssamordnare och frågat om personuppgiftsbehandlingarna som konsekvensbedömningarna grundar sig på har förändrats sedan konsekvensbedömningarna genomfördes. HR-avdelningen och beställarenheten funktionsnedsättning och socialpsykiatri har meddelat att deras behandlingar är oförändrade och konsekvensbedömningarna därmed aktuella. Avdelning Förskola har meddelat att vissa behandlingar har förändrats och att de planerar att påbörja en översyn av sina konsekvensbedömningar i januari 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 avdelning Social omsorg barn och unga och Administrativa avdelningen inte har konsekvensbedömt alla högriskbehandlingar.

3.4.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet rekommenderar att stadsdelsnämnden ger avdelningschefen för avdelning Social omsorg barn och unga och avdelningschefen för Administrativa avdelningen i uppdrag att konsekvensbedöma högriskbehandlingar under 2022.

Vidare föreslår dataskyddsombudet att stadsdelsnämnden ger dataskyddsombudet i uppdrag att följa upp att detta har genomförts och att rapportera resultatet i årsrapporten för 2022 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?	Tre.
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	En.

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. Den 5 november 2021 hade tre stycken begäran inkommit till förvaltningen. En av dessa har utretts och besvarats inom 30 dagar. I två fall har tidsfristen behövts förlängas. De registrerade har blivit informerade om anledningen till förlängningen.

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, utomstående eller registrerad.
Hur många personuppgiftsincidenter har dokumenterats?	Totalt 28 stycken.
Hur många av dessa har ansetts behöva rapporteras (till Integritetsskyddsmyndigheten respektive till berörda personer) och inte?	11 incidenter har rapporterats till Integritetsskyddsmyndigheten. 8 incidenter har informerats till berörda personer.
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Alla incidenter som har rapporterats till Integritetsskyddsmyndigheten har rapporterats i tid.

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 rapportera till 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, utomstående eller registrerade 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 22 november 2021 hade totalt 28 personuppgiftsincidenter inträffat under 2021. 11 av dessa har rapporterats vidare till Integritetsskyddsmyndigheten och rapportering har skett i tid i samtliga fall. I 8 fall har de registrerade fått information om inträffade incidenter.

De flesta personuppgiftsincidenter som inträffat i förvaltningen handlar om att uppgifter har skickats till fel mottagare, att fel uppgifter har skickats till mottagare eller att datorer eller telefoner har tappats bort eller blivit stulen. Dataskyddsombudet upplever att verksamheterna inte riktigt vet vad de ska göra vid förlust av dator eller telefon. Förvaltningen har ingen särskild skriftlig rutin för detta. Detta leder ibland till att sådana personuppgiftsincidenter kommer in sent till dataskyddsombudet.

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 någon skriftlig rutin för vad som ska göras i samband med förlust av arbetstelefon eller arbetsdator.

3.6.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet rekommenderar att stadsdelsnämnden ger informationssäkerhetssamordnaren i uppdrag att ta fram en skriftlig rutin för vad som ska göras vid förlust av arbetstelefon eller arbetsdator.

Vidare föreslår dataskyddsombudet att stadsdelsnämnden ger dataskyddsombudet i uppdrag att följa upp att detta har genomförts och att rapportera resultatet i årsrapporten för 2022 till nämnden.

4 Planerade granskningar under det nya verksamhetsåret

4.1 Sammanfattning

Under 2022 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.

Utöver det kommer dataskyddsombudet att granska att förvaltningen har en fungerande rutin för uppföljning av personuppgiftsbiträdesavtal.

4.2 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 väljer dataskyddsombudet ut ytterligare områden som ska granskas. Urvalet sker utifrån ett riskbaserat synsätt.

4.3 Planerade granskningar

4.3.1 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 2021.

4.3.2 Rutin för uppföljning av personuppgiftsbiträdesavtal

Dataskyddsombudet kommer att granska om förvaltningen har en fungerande rutin för att följa upp att personuppgiftsbiträden följer kraven i personuppgiftsbiträdesavtalen.

Dataskyddsombudet kommer först och främst att kontrollera om det finns relevanta styrdokument för detta. Därutöver kommer dataskyddsombudet att kontrollera i vilken omfattning uppföljning sker i praktiken, exempelvis genom att be relevanta avdelningar att rapportera vilka uppföljningar som har gjorts och hur man har valt ut vilka uppföljningar som ska ske.