



Stockholms
stad

GDPR Årsrapport

2021

Fastighetsnämnden

GDPR årsrapport
Januari 2022

Dnr: FSK 2021/1
Utgivningsdatum: 2022-01-19
Kontaktperson: Henrik Petersson

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 *dokumenteringsskyldighet*. Årsrapporten är även ett medel för nämnds/bolagsstyrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehåll

1	Bakgrund	3
2	Sammanfattning	5
3	Obligatoriska rapporteringsområden	6
3.1	Registerförteckning	7
3.2	Styrdokument	10
3.3	Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar	13
3.4	Konsekvensbedömningar	15
3.5	Individens rättigheter	17
3.6	Personuppgiftsincidenter	19
4	Genomförda granskningar under året	21
4.1	Sammanfattning	21
4.2	Syfte	21
4.3	Genomförda granskningar och deras resultat	21
4.4	DSO ger råd och rekommendationer till PUA	21
5	Risker inom dataskydd	22
5.1	Sammanfattning	22
5.2	Syfte	22
5.3	Resultatet av riskkartläggningen	22
5.4	DSO ger råd och rekommendationer till PUA	23
6	Planerade granskningar under det nya verksamhetsåret	24
6.1	Sammanfattning	24
6.2	Syfte	24
6.3	Planerade granskningar	24
7	Övrigt att rapportera	26
7.1	Sammanfattning	26
7.2	Syfte	26
7.3	Övriga observationer	26
7.4	DSO ger råd och rekommendationer till PUA	26

2 Sammanfattning

I egenskap av dataskyddsombud på Fastighetskontoret lämnar jag följande årsrapport.

Årets dataskyddsarbete har påverkats av att nytt dataskyddsombud tillträdde i maj. Fastighetskontoret har också genomgått en större organisationsförändring under året som trädde i kraft vid halvårsskiftet. Detta sammantaget kan delvis förklara den låga aktiviteten på dataskyddsområdet.

Att Stadsledningskontoret sent på året och med väldigt lite information till förvaltningarna helt ändrade syn på vem som kan vara dataskyddsombud aktualiserade behovet av att se över Fastighetskontorets dataskyddsorganisation. En översyn som ska vara klar under 2022 med det uttalade målet för den nya organisationen att kunna lämna en årsrapport med färre identifierade brister.

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?	67
Har nödvändiga uppdateringar gjorts?	Delvis
Bedöms registerförteckningen vara fullständig?	Oklart
Har verksamheten lämpliga rutiner för registerföring?	Nej, nya rutiner bör tas fram då ansvaret tidigare legat på DSO

3.1.2 Syfte

För att något ska gå att skydda måste det vara synligt för verksamheten. Enligt dataskyddsförordningens artikel 30 måste en personuppgiftsansvarig, inventera alla personuppgiftsbehandlingar och dokumentera dessa i ett register.

Registerförteckningen är dataskyddsarbetets centrala utgångspunkt och bas. Den är en förutsättning för att kunna säkerställa att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling. Om dokumenteringskravet uppfylls finns en grundläggande förutsättning för verksamheten att arbeta effektivt, systematiskt och riskbaserat och samtidigt värna individens integritet.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

Det finns sammanlagt 67 registrerade personuppgiftsbehandlingar i registerförteckningen.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Det finns ett behov av att uppdatera registerförteckningen, bland annat vem som är ansvarig för respektive behandling. Enligt beslut i Fastighetskontorets ledningsgrupp är det avdelningscheferna som är ansvarig för behandlingar inom deras respektive avdelning.

Samtliga avdelningschefer har vidtalats och ett antal av behandlingarna har uppdaterats under året. Några kvarstår. Målet är att samtliga personuppgiftsbehandlingar ska vara registrerade och uppdaterade under första kvartalet 2022. Även mallen för registerförteckningen behöver ses över och uppdateras. Dataskyddsombudet hade gärna sett att uppdateringen av registret skett snabbare efter att den här bristen påtalades för ansvariga avdelningschefer i september 2021.

DSO bedömer hur fullständig registerförteckningen är

Säker bedömning om hur fullständig registerförteckningen är kan ske först efter samtliga ansvariga uppdaterat sina behandlingar enligt ovan.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Nya rutiner behöver tas fram då dataskyddsombudet för närvarande är ansvarig för registret. Detta är ej förenligt med dataskyddsombudets oberoende. Vem som ska vara ansvarig för registret ingår i arbetet med att se över organisationen kring dataskyddsarbetet på Fastighetskontoret.

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

Nuvarande rutin för uppdatering av registret är ej tillfredsställande och en ny rutin behöver tas fram. Arbeta pågår med att uppdatering av registerförteckningen men tyvärr har detta dragit ut på tiden och beräknas vara klart under först under 2022.

Då registerförteckningen är en grundläggande förutsättning för dataskyddsarbetet får bristerna anses vara omfattande, särskilt mot bakgrunden att ansvariga vidtalades redan i september.

3.1.5 DSO ger råd och rekommendationer till PUA

Ny ansvarig för registerförteckningen behöver utses då dataskyddsombudet ej kan ha detta ansvar. Detta kommer ske inom arbetet med att ta fram en ny dataskyddsorganisation. Samtliga ansvariga för behandlingar behöver genomgå utbildning i vikten av att hålla registret uppdaterat.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Några styrdokument saknas
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Ja
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Ja
Är dokumenten uppdaterade?	Nej
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja, men oklarheter kring ansvaret har rått under en tid

3.2.2 Syfte

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

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?

Följande styrdokument saknas:

- **Rutin för hur verksamheten hanterar inbyggt dataskydd och dataskydd som standard i verksamhetens processer.** Skriftlig separat rutin saknas men vid inköp och införande av nya system så arbetar Fastighetskontoret efter många av de principer som utgör en bra grund för inbyggt dataskydd och dataskydd som standard. Exempelvis låsta värden och så få fritext-fält som möjligt, vilket minskar risken för att användare fyller i olämpliga personuppgifter i systemen av misstag eller okunskap. Enbart personlig inloggning med tjänstekort är tillåten i Fastighetskontorets system i enlighet med stadens riktlinjer.
- **Rutin för hur verksamheten hanterar de säkerhetsåtgärder som ska finnas för personuppgiftsbehandlingar.** Skriftlig rutin saknas, men Fastighetskontoret arbetar kontinuerligt med säkerheten och under 2021 anställdes en säkerhetschef som bland annat håller på att ta fram en ny säkerhetsskyddsanalys som delvis täcker de här frågorna.
- **Rutin för publicering av personuppgifter på stadens websidor och sociala medier.** Skriftlig separat rutin saknas men stadens centrala direktiv följs.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

Rutindokumentet håller i grunden bra kvalitet, men behöver generellt gås igenom och uppdateras. Exempelvis med nya rutiner för konsekvensbedömning och anmälan av personuppgiftsincident till Integritetsskyddsmyndigheten.

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

Arbete med att se över dataskyddsorganisationen och ansvaret för styrdokumenterna pågår. De befintliga styrdokumenterna håller bra kvalitet. Att vissa skriftliga rutiner saknas utgör ingen allvarlig risk då det i stor mån redan arbetas efter bra dataskyddsprinciper.

3.2.5 DSO ger råd och rekommendationer till PUA

Ägarskap för samtliga styrdokument behöver fastställas, vilket sker i samband med översyn av organisationen. Saknade styrdokument ska upprättas/inkluderas i befintliga rutiner. Befintliga styrdokument behöver gås igenom och vid behov uppdateras.

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?	Samtliga
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 Syfte

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

3.3.3 Resultat

Informationsklassning utifrån ett GDPR-perspektiv är genomförd på samtliga personuppgiftsbehandlingar under 2020 och 2021 vilket innebär att de är aktuella enligt stadens riktlinjer.

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

Informationsklassning är genomförd och aktuell.

3.3.5 DSO ger råd och rekommendationer till PUA

Inga speciella råd eller rekommendationer.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Ja, utifrån registerförteckningen som den ser ut idag
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Ja
Är de genomförda bedömningarna aktuella?	En översyn bör göras

3.4.2 Syfte

Konsekvensbedömning av en personuppgiftsbehandling hjälper personuppgiftsansvarig att identifiera och minimera integritetsriskerna för de uppgifter 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 kan/ska riskförebyggande åtgärder vidtas. Konsekvensbedömningen anses liksom registerförteckning och informationsklassning vara 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) Det är alltså inte nödvändigt med en konsekvensbedömning av samtliga personuppgiftsbehandlingar, men en initial riskbedömning ska alltid göras och dokumenteras.

3.4.3 Resultat

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

Eftersom identifiering av högriskbehandlingar är beroende av en uppdaterad registerförteckning över behandlingar går det ej att

besvara frågan med 100% säkerhet förrän registerförteckningen är fullständigt uppdaterad (se kapitel 3.1 i denna rapport).

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Samtliga nu identifierade högriskbehandlingar i registerförteckningen har konsekvensbedömts.

Är de genomförda konsekvensbedömningarna aktuella?

Även den här frågan är beroende av en uppdaterad registerförteckning, men utifrån nuvarande information i registerförteckningen är konsekvensbedömningarna aktuella.

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

Utförda konsekvensbedömningar behöver ses över.

3.4.5 DSO ger råd och rekommendationer till PUA

Utförda konsekvensbedömningar behöver ses över, men det behöver inte ske mer brådskande än den pågående generella översynen av dataskyddsarbetet i stort på Fastighetskontoret.

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 även ha viss kontroll över personuppgiftsbehandlingen. Det är ett krav enligt förordningen att personuppgiftsansvarig tillgodoser rättigheterna.

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

Ja.

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

Inga risker identifierade.

3.5.5 DSO ger råd och rekommendationer till PUA

Övervaka så att möjligheterna att tillgodose individens rättigheter ej försämras.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Genom medarbetare
Hur många personuppgiftsincidenter har dokumenterats?	1
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	0
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	N/A

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.”

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland dataskyddsförordningens olika verktyg för att åstadkomma en sund personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering.

3.6.3 Resultat

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

En incident har inträffat och den har hanterats korrekt.

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

Ingen brist identifierad

3.6.5 DSO ger råd och rekommendationer till PUA

Med bara en enda incident är underlaget för litet för att kunna dra några djupgående slutsatser. Incidenthantering är en så pass viktig och central del i dataskyddsarbetet att det under 2022 bör säkerställas att styrdokumenterna är uppdaterade och att samtliga medarbetare är medvetna förvaltningens rutiner.

4 Genomförda granskningar under året

4.1 Sammanfattning

Inga granskningar har genomförts under året.

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.

4.3 Genomförda granskningar och deras resultat

Inga granskningar har genomförts under året.

4.4 DSO ger råd och rekommendationer till PUA

När den nya dataskyddsorganisationen är beslutad ska granskningsverksamheten återupptas.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- Organisering och struktur
- Personuppgiftsbiträden

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.

5.3 Resultatet av riskkartläggningen

Komplett riskkartläggning är ej gjord, men några risker har observerats under året.

Risk 1

Risk inom intern organisering och struktur, en fullständig dataskyddsorganisation har saknats och dataskyddsarbetet har ej varit prioriterat under en tid. En översyn av dataskyddsorganisationen och dataskyddsarbetet i stort är pågående.

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

Risk 2

Risk inom hantering av personuppgiftsbiträden, det råder viss oklarhet om rutinen för personuppgiftsbiträdesavtal (PUB-avtal) följs och om det finns avtal för samtliga biträden.

	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

5.4 DSO ger råd och rekommendationer till PUA

Etablera en ändamålsenlig dataskyddsorganisation med klart ansvar för samtliga roller inklusive dataskyddsombudet. Se även över behovet av utbildning och förtydligande kring processen för att teckna PUB-avtal.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Register över personuppgiftsbehandlingar
- Personuppgiftsbiträden
- Hantering och rapportering av personuppgiftsincidenter

6.2 Syfte

Det granskande arbetet är en av dataskyddsombudets viktigaste uppgifter. Efter att granskningsverksamheten legat i träda under lång tid, sedan före nuvarande dataskyddsombud tillträdde, så är det av vikt att minst tre granskningar genomförs under 2022.

6.3 Planerade granskningar

Granskning 1

Registerförteckningen över personuppgiftsbehandlingar är grunden i dataskyddsarbetet, vi måste veta vilka behandlingar som finns för att kunna skydda personuppgifterna. Ett arbete med att se över och uppdatera registret pågår på förvaltningen (se kapitel 3.1 i denna rapport). Granskningen ska fokusera på om registret är komplett och om samtliga uppgifter är aktuella.

Granskning 2

Rutin för personuppgiftsbiträden och personuppgiftsbiträdesavtal ska uppdateras under 2022. Personuppgiftsombudet ska granska uppdateringarna. Även granska så att det finns avtal för samtliga personuppgiftsbiträden och att uppföljningar görs.

Granskning 3

Rutiner för personuppgiftsincidenthantering ska uppdateras under 2022. Efter uppdatering ska de granskas av personuppgiftsombudet för att se att uppdateringarna är korrekta. Även se över kunskapsläget i stort så att förvaltningen kan vara säker på att incidenter upptäckts och rapporteras i enlighet med rutinerna. Finns

det några rapporterade incidenter ska dataskyddsombudet granska dessa för att se om rutinerna följts.

7 Övrigt att rapportera

7.1 Sammanfattning

Dataskyddsbudeten på Fastighetskontoret har synpunkter på hur Funktionen för stadsövergripande informationssäkerhet vid Stadsledningskontoret kommunicerar ställningstaganden som påverkar de enskilda förvaltningarnas dataskyddsarbete.

7.2 Syfte

Avsikten med denna punkt i årsrapporten är att ta upp synpunkter och observationer som inte passar in under tidigare avsnitt.

7.3 Övriga observationer

Observation 1

Funktionen för stadsövergripande informationssäkerhet vid Stadsledningskontoret uttryckte sent 2021 sin uppfattning att det inte är lämpligt att kombinera en roll som arkivarie med en roll som dataskyddsbudeten. Yrkesrollerna arkivarie och dataskyddsbudeten kombineras på många förvaltningar, däribland Fastighetskontoret. Detta ställningstagande kommunicerades enbart i en fotnot i instruktionerna till verksamhetsplanen för 2022. Ingen annan kommunikation eller dialog kring denna uppfattning har förts med någon förvaltning såvitt är känt.

Observationen ligger utanför Fastighetsnämndens som personuppgiftsansvarigs område, men bör ändå uppmärksammas då Stadsledningskontorets ställningstagande påverkar Fastighetskontorets dataskyddsarbete.

7.4 DSO ger råd och rekommendationer till PUA

Då observationen ligger utanför Fastighetsnämndens ansvar som personuppgiftsansvarig så finns det ingen direkt rekommendation.