Stockholms stad

GDPR Årsrapport

År 2023

Fastighetsnämnden

GDPR årsrapport
2023

Dnr:
Utgivningsdatum: 2023-12-29
Kontaktperson: Alexandre Emonide

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 privatliv och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. GDPR syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

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

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

Denna årsrapport syftar till att redogöra för de granskningar som gjorts under året. Rapporten avslutas med rekommendationer för det fortsatta dataskyddsarbetet.

Innehåll

2 Sammanfattning

DSO lämnar följande årsrapport.
Denna rapport är sammanställd av DSO i syfte att ge personuppgiftsansvarig (PUA), i Fastighetskontorets fall är det fastighetsnämnden, en redogörelse för hur dataskyddsarbetet har genomförts på Fastighetskontoret under 2023. Fastighetskontoret har viktiga delar som behöver komma på plats gällande dataskyddsarbetet. Det finns en registerförteckning som behöver uppdateras löpande. En identifierad brist är avsaknad av styrdokument som leder till bristande kvalitet i hur verksamheten utför aktiviteter. Vidare behöver rutiner tydliggöras för hur dataskyddsarbetet ska ske löpande i verksamheten
Ytterligare en brist är avsaknaden av konsekvensbedömningar. En insats gällande arbetet med konsekvensbedömningar har påbörjats under 2023 och detta arbete bör följas upp under 2024. En utbildningsinsats är planerad under våren 2024. Det finns vidare en del organisatoriska brister som leder till att en del av ansvaret gällande dataskyddsarbetet hamnar hos DSO, vilket är olämpligt eftersom DSO främst ska ha en granskande oberoende roll.

2.1 Översiktlig bedömd status för rapporteringsområden

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

(För specificering se respektive avsnitt)

3 Obligatoriska rapporteringsområden

Denna årsrapport redogör för sex obligatoriska rapporteringsområden. Dessa områden ska ses över årligen av personuppgiftsansvarig (”PUA”) i syfte att efterleva GDPR.

De obligatoriska rapporteringsområdena är följande

- registerförteckning
- styrdokument
- tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar
- konsekvensbedömningar
- individens rättigheter och personuppgiftsincidenter
- Personuppgiftsbiträdesavtal

Nedan redogörs för Fastighetskontoret status och DSO:s slutsatser samt rekommendationer.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	67
Har verksamheten rutiner som möjliggör att nya/förändrade personuppgiftsbehandlingar registreras?	Delvis
Bedöms registerförteckningen vara fullständig?	Delvis
Har verksamheten lämpliga rutiner för registerföring?	Delvis

3.1.2 Syfte

Förteckning på behandlingar, även kallad registerförteckning eller behandlingsregister, är ett direkt lagkravkrav enligt GDPR. Kravet innebär att samtliga behandlingar av personuppgifter ska kartläggas i en förteckning/register. Informationen i förteckningen/registret ska hållas uppdaterad, aktuell och komplett och granskas av DSO. Syftet med detta avsnitt är att granska Fastighetskontorets förteckning/register.

3.1.3 Resultat

I dagsläget finns 67 personuppgiftsbehandlingar registrerade i registerförteckningen.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Registerförteckningen måste uppdateras regelbundet. Vissa justeringar är gjorda under året men den senaste registrerade uppdateringen gjordes under våren 2023.

DSO bedömer hur fullständig registerförteckningen är

Registerförteckningen är omfattande men eftersom den inte uppdaterats regelbundet kan det inte fastställas om den är fullständig. Vissa behandlingar saknas och vissa saknar en angiven informationsägare.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Det saknas tydliga rutiner för hur, när och av vem registerförteckningen ska uppdateras. I dagsläget tycks uppdateringar ske främst på uppmaning från DSO.

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

3.1.5 DSO ger råd och rekommendationer till PUA

Systemet DraftIT Privacy Records gör det enklare att uppdatera registerförteckningen vilket bidrar till att uppdateringar görs mer löpande efter hand som nya eller förändrade personuppgiftsbehandlingar införs i verksamheten. Det bör göras en omfattande genomgång av registerförteckningen och nya rutiner för hur uppdateringar av registerförteckningen ska ske tas fram. Ansvariga för att hålla registerförteckningen uppdaterad är informationsägarna, oftast avdelningscheferna, men även processledare bör medverka både vid uppdateringen av registerförteckningen och vid framtagandet av rutiner då dessa har god insyn i verksamheten.

Ett tillägg i rekommendationen är att nuvarande inventering lämnas oförändrad och att endast nya eller ändrade behandlingar registreras i Draftit. Stadens mall i Draftit kan användas för inventeringar och ingen ny mall behöver tas fram. En översyn av nuvarande

inventering i Draftit har genomförts i maj 2023 för att kunna avgöra om registerförteckningen är fullständig.

DSO rekommenderar Fastighetskontoret att påbörja arbetet med att ta fram en ny mall för inventering av personuppgiftsbehandlingar utifrån systemperspektiv i början på år 2024.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Delvis
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Ja
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Delvis
Är dokumenten uppdaterade?	Stadens gemensamma styrdokument uppdateras centralt.
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ägare för centrala styrdokument finns.

3.2.2 Syfte

Exempel på styrdokument är, mall för personuppgiftsbiträdesavtal, incidenthanteringsrutin och rutin för registerutdrag. Styrdokument ska finnas nedtecknade, beslutade och kommunicerade. Genom styrdokument kommuniceras till medarbetarna vad som förväntas av dem samt information om regler, ramar och förutsättningar och stöd för att upprätthålla kunskapen över tid och tillämpa den på ett konsekvent sätt. Syftet med detta avsnitt är att granska Fastighetskontorets styrdokument.

3.2.3 Resultat

Rapporteringen delas upp i två delar: dels ska DSO bedöma om verksamheten har styrdokument på plats, dels ska rapporteringen

visa om dokumentationen innehållsmässigt håller en lämplig kvalitet, i vilket bland annat ingår att dokumentationen ska vara uppdaterad och aktuell. En brist inom detta område bör ses som en brist i förhållande till direkta lagkrav, men det finns fler nyanser av detta som bör lyftas fram till PUA. Avsaknad av styrande dokumentation leder ofta till bristande kvalitet i hur verksamheten bedrivs samt till att verksamheten slösar värdefulla resurser när för många medarbetare blir involverade i exempelvis en incidenthantering. Ytterligare ett exempel på ineffektivt och bristande arbetssätt är när analyser görs om från grunden varje gång i stället för att ha styrdokument att utgå ifrån vid behov.

Finns lämplig styrande dokumentation på plats?

Verksamheten utgår från centralt framtagna styrdokument. Verksamhetsanpassade styrdokument saknas.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

DSO bedömer att det bör göras en översyn över vilka styrdokument som saknas och vad som behövs revideras kommande år.

3.2.4 DSO anger hur allvarliga bristerna är på en skala

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

3.2.5 DSO ger råd och rekommendationer till PUA

Den dokumentation som finns är inte uppdaterad och anpassad till Fastighetskontorets verksamhet. Det finns också vissa frågetecken kring hur kännedomen bland medarbetarna är kring dessa styrdokument. Den dataskyddsorganisation som finns fastställd behöver uppdateras och vidareutvecklas för att kunna användas praktiskt i verksamheten.

DSO rekommenderar att en översyn av samtliga styrdokument görs under 2024 för att identifiera vilka dokument som behöver kompletteras eller tas fram.

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?	Alla
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 Syfte

Tekniska och organisatoriska säkerhetsåtgärder är grunden till ett bra informationssäkerhetsarbete. Tekniska och organisatoriska säkerhetsåtgärder ska därför vara en del av organisationens arbete.

Tekniska säkerhetsåtgärder innefattar främst IT-säkerhet och systemsäkerhet. Organisatoriska säkerhetsåtgärder innefattar det systematiska GDPR-arbetet i form av rutiner, instruktioner analyser och regelefterlevnad.

Syftet med detta avsnitt är att granska Fastighetskontorets tekniska och organisatoriska säkerhetsåtgärder samt att ge rekommendationer kring det fortsatta arbetet.

3.3.3 Resultat

Alla personuppgiftsbehandlingar har informationsklassats och är aktuella.

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

3.3.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att en genomgång av de befintliga informationsklassningarna från 2023 görs av respektive informationsägare i samråd med DSO avseende personuppgiftsbehandlingen och med hjälp av informationssäkerhetssamordnare för att utreda om ytterligare klassning ur ett informationssäkerhetsperspektiv behövs för dessa behandlingar. I samband med uppdateringen av registerförteckningen bör tillfälle ges att identifiera ytterligare behandlingar som ska klassas. DSO rekommenderar att en genomgång av detta görs i samband med översynen av registerförteckningen.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?	Ja
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?	Ja
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd genomförs samt genomfört detta?	Nej
Finns det en ändamålsenlig mall samt för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?	Rutin för tröskelanalys har tagits fram och två konsekvensbedömningar har gjorts enligt stadens mall.

3.4.2 Syfte

Syftet med att göra konsekvensbedömningar är att förebygga risker för att skydda de registrerade och att efterleva GDPR. En konsekvensbedömning är en bedömning av de konsekvenser som kan uppstå när man behandlar personuppgifter. I bedömningen tar man ställning till om risken är proportionerlig i förhållande till ändamålet med behandlingen av uppgifterna. Visar det sig att risken är för hög för att motivera ändamålet kan bedömningen resultera i att det inte går att genomföra behandlingen, alternativt tas åtgärder fram för att sänka risken. En konsekvensbedömning ska även genomföras om det föreligger risker då en behandling förändras.

Syftet med detta avsnitt är att granska Fastighetskontorets rutin för konsekvensbedömningar samt att ge rekommendationer kring det fortsatta arbetet.

3.4.3 Resultat

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

Nej, ingen övergripande genomgång har gjorts för att identifiera om det finns fler behandlingar som behöver konsekvensbedömmas. Arbetet med att identifiera personuppgiftsbehandlingar som kräver en konsekvensbedömning pågick löpande under första halvan av året. För perioden september-december 2023 har inga personuppgiftsbehandlingar som kräver en konsekvensbedömning identifierats.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

För perioden september-december 2023 har inga högriskbehandlingar identifierats.

Är de genomförda konsekvensbedömningarna aktuella?

För perioden september-december 2023 har inga högriskbehandlingar varit 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

3.4.5 DSO ger råd och rekommendationer till PUA

Rutin för tröskelanalys har tagits fram och två konsekvensbedömningar har gjorts enligt stadens mall. Även en översyn av alla behandlingar har genomförts för att identifiera behandlingar som kräver en konsekvensbedömning. Översynen resulterade i en behandling som enligt tröskelanalysen hade en rekommendation om att göra en fullständig konsekvensbedömning.

Konsekvensbedömningen för den behandlingen gjordes våren 2023. DSO rekommenderar ett fortsatt arbete under första kvartalet 2024.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?	Ja
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	0
Hur många av de inkomna begärandena har besvarats av verksamheten inom 30 dagar?	0

3.5.2 Syfte

Individens rättigheter regleras i flera artiklar i GDPR. Några rättigheter som kan nämnas är den registrerade rätt att begära och få registerutdrag, rätt till rättelse samt rätt till radering.

Syftet med detta avsnitt är att granska Fastighetskontorets dokumentation och arbetsmaterial gällande individens rättigheter samt att ge rekommendationer kring det fortsatta arbetet.

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

För år 2023 har ingen begäran om registerutdrag 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
x	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.5.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar Fastighetskontoret att uppdatera befintliga mallar och rutiner för att enkelt kunna besvara begäran från den registrerade.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur säkerhetsställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftincident?	Arbete pågår
Finns det rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter samt följs dessa?	Arbete pågår
Hur många personuppgiftincidenter har anmälts till IMY?	0
Hur många personuppgiftsincidenter har dokumenterats?	1

3.6.2 Syfte

Att identifiera och hantera personuppgiftsincidenter är ett direkt krav i GDPR. Det är även viktigt att aktivt arbeta med att förebygga

personuppgiftsincidenter för att spara tid och resurser samt för att bygga en riskmedveten säkerhetskultur i verksamheten.

Syftet med detta avsnitt är att granska Fastighetskontorets rutiner och processer gällande personuppgiftsincidenter samt att ge rekommendationer kring det fortsatta arbetet.

3.6.3 Resultat

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

Nuvarande rutin för rapportering av personuppgiftsincidenter behöver ses över och eventuellt förtydligas i verksamheten.

3.6.4 DSO anger hur allvarliga bristerna är på en skala

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

3.6.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar Fastighetskontoret att arbeta med rutinen för personuppgiftsincidenthantering tillsammans med medarbetarna i samband med en föreläsning/workshop under våren 2024. Detta för att göra rutinen etablerade i verksamheten och höja medvetenheten om incidenthantering. Vidare har det förts diskussioner om att ersätta IA som rapporteringssystem för personuppgiftsincidenter, dock finns det i nuläget inga andra alternativ.
Ett arbete med utbildning/informationsinsatser planeras under våren 2024.

4 Genomförda granskningar under året

4.1 Sammanfattning

Få granskningar genomfördes under perioden september-december 2023 då DSO på grund av behörighetsproblematik haft en begränsad insyn i verksamheten. DSO har inte haft tillgång till material och systemet DraftIT Privacy Records.

4.2 Syfte

DSO ska i sitt arbete göra återkommande granskningar av hur väl GDPR efterlevs i verksamheten. Resultaten av granskningarna ligger sedan till grund för vilka beslut verksamheten fattar i fråga om dataskyddsåtgärder. För PUA är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under det gångna året och resultatet av granskningarna.

4.3 Genomförda granskningar och deras resultat

4.3.1 Styrdokument

	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 pågår.

4.4 DSO ger råd och rekommendationer till PUA

4.4.1 Styrdokument

DSO rekommenderar att en översyn av samtliga styrdokument görs år 2024 för att identifiera vilka dokument som behöver kompletteras eller tas fram.

5 Risker inom dataskydd

5.1 Sammanfattning

Nuvarande DSO har under den korta tiden inte kunnat observera några risker inom arbetet med dataskydd. Det är okänt om några riskkartläggningar har gjorts under första halvan av år 2023. DSO har haft en begränsad insyn i verksamheten vilket i sig är en risk då granskning av regelefterlevnaden uteblir.

5.2 Syfte

Verksamheten har ansvar för att göra vissa typer av riskanalyser, så som konsekvensbedömningar och informationsklassningar, dessa ger dock inte en heltäckande bild av personuppgiftsriskerna i verksamheten. DSO behöver ha kontinuerlig överblick över dessa risker, i verksamhetens samtliga personuppgiftsbehandlingar. Exempelvis krävs en sådan överblick för att kunna välja ut vilka områden som bör granskas under det kommande året eller för att avgöra vilka råd som DSO behöver lämna till verksamheten om de dataskyddsåtgärder som behöver vidtas.

5.3 DSO ger råd och rekommendationer till PUA

Rekommendation 1
Utbildningsinsatser till målgrupper som arbetar mest med personuppgifter bör genomföras under våren 2024. En informationsinsats för nämndens upphandlingsenhet ägde rum under våren 2023 och det framgick då att det finns ett behov av att förtydliga vad som gäller kring tecknande av personuppgiftsbiträdesavtal. Under våren planerade och genomfördes korta informationsinsatser för särskilda

ledningsgrupper eller arbetsplatser med dåvarande DSO. Denna insats ska fortsätta under våren 2024.

Rekommendation 2
I årsrapporten för 2022 framgår att en granskning av personuppgiftsincidenter har genomförts. Granskningen visade att rutinen för rapportering är relativt okänd i verksamheten. Rapporteringen görs i IA som är ett HR-verktyg för arbetsmiljö och inte ett anpassat verktyg för rapportering av personuppgiftsincidenter. Fram tills dess att ett nytt arbetssätt för rapportering av personuppgiftsincidenter finns på plats behöver nuvarande rutin göras känd i verksamheten, förslagsvis genom de utbildningsinsatser som planeras till våren 2024.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning
Relevanta granskningsområden inom verksamheten:

- Styrdokument
- Registerförteckning och Konsekvensbedömningar
- Personuppgiftsincidenter
- Årshjulsplanering för ett mer systematiskt och kontinuerligt dataskyddsarbete.

6.2 Syfte
Som nämnts ovan är det granskande arbetet en av DSO:s viktigaste uppgifter. Eftersom DSO har begränsat med tid, behöver granskningsplanen för det nya året utformas med eftertanke. Som en tumregel bör två-tre granskningar ses som en rimlig granskningsinsats under ett verksamhetsår. Granskningsområdena bör lämpligen väljas utifrån ett riskbaserat synsätt, det vill säga att fokus bör ligga på områden där verksamhetens mest relevanta risker har identifierats i en riskanalys och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Därmed följer en röd tråd i dataskyddsarbetet från ett verksamhetsår till nästa samtidigt som de största riskerna elimineras eller sänks.

6.3 Planerade granskningar

6.3.1 Styrdokument

DSO rekommenderar en översyn av samtliga styrdokument under 2024 för att identifiera vilka dokument som behöver kompletteras eller tas fram.

6.3.2 Registerförteckning och Konsekvensbedömningar

Rutiner för tröskelanalys och konsekvensbedömning har tagits fram och konsekvensbedömningar gjordes enligt stadens mall under första kvartalet 2023 tillsammans med dåvarande DSO. Under första kvartalet 2024 kommer en större granskning och genomgång av registerförteckning och konsekvensbedömningar att göras för att se om de brister som beskrivits i denna rapport har åtgärdats. DSO kommer även att ha en rådgivande funktion under arbetets gång med att åtgärda bristerna.

6.3.3 Personuppgiftsincidenter

Ett arbete med utbildning/informationsinsatser planeras under våren 2024, för att öka kunskapen och förståelsen för vad en personuppgiftsincident är.

6.3.4 Årshjulsplanering för ett mer systematiskt och kontinuerligt dataskyddsarbete

Årshjulsplanering bygger på att arbetet inom dataskyddet delas upp i ett årshjul, där varje månad är indelad i ett fokusområde. I årshjulet delas arbetsuppgifterna upp i löpande aktiviteter som utvärderas, granskas och förbättras. Årshjulet är ett effektivt sätt att strukturera arbetet på. Årshjulet innebär även ett bra sätt att fördela arbetet mellan DSO och Dataskyddsorganisationen. Genom att arbeta strukturerat med årsrapport och granskning kan man följa Fastighetskontorets utveckling under en längre tid.

7 Övrigt att rapportera

7.1 Övriga observationer

Observation 1

Tidigare DSO har tillsammans med tidigare dataskyddsamordnare planerat för en satsning inom arbetet med dataskydd under första perioden av 2023, dock avtog takten i arbetet i och med att dataskyddsamordnaren avslutade sin anställning samtidigt som kontoret fick ett nytt DSO. Det i kombination med att ny DSO på grund av behörighetsproblematik haft en begränsad insyn i verksamheten har resulterat i ett glapp i dataskyddsarbetet. Datatskyddsarbetet behöver stabiliseras samt få upp farten framåt.

Observation 2

Fastighetskontorets verksamhet behandlar sällan stora mängder känsliga personuppgifter och fokus har varit att se över registerförteckningen, hantering av personuppgiftsincidenter och information kring tecknande av personuppgiftsbiträdesavtal. Ansvariga för de befintliga PUB-avtalen, oftast avdelningschefer, bör gå igenom avtalen för att se om de behöver kompletteras.

7.2 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att till nästa årsrapport läggs in ytterligare ett rapporteringsområde - Överföring till tredje land
Förslag på frågor:

- Har personuppgiftsansvarig identifierat tredjelandsöverföringar?
- Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?
- Har nödvändig bedömning, så kallad ”Transfer Impact Assessment (TIA), gjorts avseende de tredjelandsöverföringar som utförs?