Stockholms stad

Bilaga 13

GDPR Årsrapport

År 2023

Exploateringsnämnden

GDPR årsrapport
Januari 2023

Dnr: E2022-05671
Utgivningsdatum: 2023-01-23
Kontaktperson: Patrik Stensson

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 Dataskyddsombud för exploateringsnämnden lämnar jag följande årsrapport.

Det är exploateringsnämnden som är PUA, men samtidigt är det exploateringskontoret som utför uppgifterna i dataskyddsarbetet, därför kommer exploateringskontoret fortsättningsvis att vara den beteckning som används för PUA i denna rapport.

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?	174
Har nödvändiga uppdateringar gjorts?	Delvis
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

Enligt Dataskyddsförordningen ska personuppgiftsansvarig föra ett register över samtliga personuppgiftsbehandlingar (artikel 30). Det är en viktig del av ansvarsskyldigheten, det vill säga att kunna visa att personuppgiftsansvarig följer Dataskyddsförordningen (artikel 5.2).

Att föra register är ett av de viktigaste verktygen i dataskyddsarbetet och granskning av registret är en av de viktigaste delarna av DSO:s arbete med uppföljning av dataskyddet på exploateringskontoret.

3.1.3 Resultat

Exploateringskontoret har för närvarande 176 registrerade behandlingar.

Exploateringskontoret har inventerat lokala och centrala system och lagt till ytterligare processer.

Exploateringskontoret för registret i en excel-fil, men planerar att föra över uppgifterna i Sharepointlista som blir en del av Ledningssystemet för informationssäkerhet (LIS). Objektledare/informationsägare kan själv uppdatera listan.

Exploateringskontoret kommer att utarbeta tydliga rutiner för hur och av vem redan pågående och planerade behandlingar ska registreras och uppdateras.

Dataskyddsansvarig ser över registret en gång i kvartalet.

Registret är inte fullständigt, det är ett pågående arbete.

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

3.1.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att exploateringskontoret fortsätter att uppdatera registret och utbilda Objektledare/informationsägare i hur man uppdaterar registret.

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?	Ja
Är dokumenten uppdaterade?	Delvis
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja

3.2.2 Syfte

Att ha styrdokument, riktlinjer och rutiner på plats är tillsammans med registret en viktig del av ansvarsskyldigheten, det vill säga att exploateringskontoret/PUA ska kunna visa att det följer Dataskyddsförordningen.

3.2.3 Resultat

Exploateringskontoret har en riktlinje för personuppgiftshantering från 2021-10-01. Denna ska uppdateras under 2024.

Incidenthanteringsrutin är framtagen.

Exploateringskontoret ska ta fram en allmän information om personuppgiftbehandlingar på stadens webb.

Exploateringskontoret arbetar med att ta fram en mall för information till de registrerade.

Exploateringskontoret följer stadens riktlinje för informationssäkerhet och använder stadens protokoll för informationsklassning och riskbedömning KLASSA 4.

Lokal tillämpningsanvisning för informationssäkerhet kommer att tas fram.

Dokumentet Ledningens genomgång år 2023 (Verksamhetsplan 2024 bilaga 2:1) har tagits fram.

Ledningssystem för informationssäkerhet (LIS) kommer att införas med tillhörande styrdokument, riktlinjer och liknande.

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

DSO rekommenderar att de dokument som planerats och påbörjats slutförs och implementeras.

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

Informationsklassning är en metod att bedöma risk och åtgärder för att komma tillrätta med risker med informationshanteringen. Bland de frågor som ställs i klassningen finns det specifika frågor som rör dataskyddet. Därför är det mycket viktigt att all information som ägs av exploateringskontoret klassas, då kommer dataskyddsfrågorna automatiskt att behandlas. Bland annat frågan om det är nödvändigt med en konsekvensbedömning. Även frågor om registret, de registrerades rättigheter, säkerhetsåtgärder och tredjelandsöverföringar ställs här.

3.3.3 Resultat

Exploateringskontoret har informationsklassat samtliga informationsmängder.

I personuppgiftsbehandlingsregistret anges i nuläget inte vilka behandlingar som har genomgått en informationsklassning.

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 exploateringskontoret fortsätter att informationsklassa tillkommande informationsmängder.

DSO rekommenderar att exploateringskontoret anger i registret att informationsklassning har utförts.

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?	Ja
Är de genomförda bedömningarna aktuella?	Ja

3.4.2 Syfte

Om risken för de registrerades fri och rättigheter bedöms som hög utifrån de kriterier som Dataskyddsförordningen anger och som Integritetsskyddsmyndigheten (IMY), som är tillsynsmyndighet för dataskyddsområdet, preciserar i en lista på sin hemsida, ska en konsekvensbedömning genomföras (artikel 35 och 36).

Om det kvarstår risker efter en konsekvensbedömning ska IMY kontaktas för förhandssamråd. Detta görs via ett webbformulär på dess hemsida.

DSO ska alltid finnas med för övervakning av genomförandet och rådfrågning.

3.4.3 Resultat

Exploateringskontoret har inte genomfört några konsekvensbedömningar under 2023.

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

3.4.5 DSO ger råd och rekommendationer till PUA

DSO har inga särskilda rekommendationer.

3.5 Individens (de registrerades) rättigheter

3.5.1 Sammanfattning

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

3.5.2 Syfte

Dataskyddsförordningen ger de registrerade vissa rättigheter som formuleras i kapitel III, dessa är:

- Rätt till information
- Rätt till tillgång (registerutdrag)
- Rätt till radering
- Rätt till rättelse
- Rätt till invändning
- Rätt till begränsning
- Rätt till dataportabilitet

Den registrerade har rätt att få ett svar inom 30 dagar, om vi inte kan visa att vi behöver längre tid. Besluten kan överklagas till allmän domstol.

3.5.3 Resultat

Exploateringskontoret har förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist. Exploateringskontoret har mycket få begäranden.

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

3.5.5 DSO ger råd och rekommendationer till PUA

DSO ha inga särskilda rekommendationer.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

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

3.6.2 Syfte

Enligt 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.”

Personuppgiftsincidenterna ska anmälas till tillsynsmyndigheten inom 72 timmar från upptäckt om exploateringskontoret inte bedömer att det är en mycket liten risk för de registrerades rättigheter och friheter.

Exploateringskontoret ska ändå anmäla och dokumentera dessa lokalt enligt stadens och kontorets rutiner.

Det kan krävas att de registrerade måste informeras. Det är om incidenten sannolikt leder till hög risk för den registrerades rättigheter och friheter.

3.6.3 Resultat

Exploateringskontoret har rutinen att rapportera i stadens IA-system.

Rutinen för incidentrapportering måste hållas aktuell genom introduktion för nyanställda och på annat sätt.

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

3.6.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att exploateringskontoret säkerställer att alla medarbetare känner till hur man rapporterar en personuppgiftsincident.