Stockholms stad

GDPR Årsrapport

2024

SGA Fastigheter AB

GDPR årsrapport
Januari 2025

Dnr: SGAF 2025/2
Utgivningsdatum: 2024-02-01
Kontaktperson: Sara Feinberg SGAF/Simon Jernelöv JPinfonet

1 Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

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

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

Denna årsrapport är således ett medel för nämnd och styrelse att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnd eller bolagsstyrelse ska kunna *visa* att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna *dokumenteringsskyldighe*t. Årsrapporten är även ett medel för nämnds/bolagsstyrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehåll

2 Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

SGA Fastigheter har god ordning på personuppgifter och bra rutiner för hantering av dessa. Bolaget behandlar relativt få personuppgifter, främst hänförande till den egna personalen samt inloggningsuppgifter (som inte anses känsliga eller integritetskänsliga enligt regelverket).

Ett större omtag av artikel-30-registret (registerförteckningen) med en tydligare struktur, och med tydligare koppling till bolagets verksamhetsprocesser, gjordes i slutet av 2021, med ytterligare arbete under 2023. Under 2024 har det skett ytterligare genomgång av denna, med rekommendationer som förväntas leda till förenklad hantering.

Bolaget hade under 2021 en fördjupad granskning från Stadsrevisionen gällande dataskydd. Granskningen visade att det finns utmaningar kopplade till DSO:s oberoende då denne varit operativ vid bland annat uppdatering av registerförteckning. I en liten organisation är det ständiga utmaningar med att bemanna alla roller. Under 2024 har istället ett externt DSO anlitats genom JP Infonet AB, för att säkerställa DSO oberoende.

Denna rapport innehåller ingen sekretessklassad information.

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 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 (verksamhetsprocesser) som är registrerade?	165
Har nödvändiga uppdateringar gjorts?	Ja
Bedöms registerförteckningen vara fullständig?	Ja
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

Under de senaste åren har bolaget arbetat med att förtydliga sin registerförteckning enligt dataskyddsförordningens artikel 30, där samtidiga personuppgiftshanteringar finns dokumenterade. Den uppdateras löpande vid behov, t.ex. systembyte.

Registerförteckningen överensstämmer numera, i stort, med bolagets klassificeringsstruktur (styrdokument inom arkiv och registratur), vilket underlättar informationshanteringen för bolaget. I bolagets registerförteckning är ’verksamhetsprocess’ och ’behandling’ särskilda, varför vi redogör för antalet genom uppdelningen nedan.

I registerförteckningen finns följande antal processer och behandlingar:
Verksamhetsområden, antal: 3 stycken
Verksamhetsprocesser (övergripande nivå), antal: 18
Verksamhetsprocesser (underliggande nivå), antal: 35
Antal identifierade behandlingar: 165

Bolaget har relativt få personuppgiftsbehandlingar, då bolaget endast har ett fåtal hyresgäster som samtliga är aktiebolag. Viss personuppgiftsbehandling sköts av hyresgästen Stockholm Live, och dessa regleras genom ett personuppgiftsbiträdesavtal (PuB-avtal).

Främst gäller personuppgiftsbehandlingen egen personal och vissa uppgifter är känsliga enligt förordningen, t.ex. sjukdom, facklig tillhörighet och religiös övertygelse.

3.1.3 Resultat

DSO har vid kontroller inte upptäckt några brister i bolagets registerförteckning.

Bolaget har i sin registerförteckning 165 möjliga behandlingar och 35 verksamhetsprocesser. Det bedöms i dagsläget inte finnas några ytterligare behandlingar som behöver registerföras.

Uppdateringar görs löpande, vid t.ex. systembyte. I bolagets lönesystem finns personuppgifter, även känsliga sådana. I övrigt behandlas främst uppgifter till användare som krävs för inloggning. Bolagets registerförteckning anses var fullständig.

Bolagets rutiner för registerföring fungerar bra.

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

Bolaget har bra rutiner för personuppgiftshantering. Inga brister har upptäckts. Det är dock nödvändigt att bolaget fortsätter att följa upp personuppgiftshanteringen samt att registerförteckningen löpande hålls uppdaterad, exempelvis genom att rutiner för detta inkluderas i årshjulet för bolagets kvalitetsarbete.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Ja
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Ja
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Ja
Är dokumenten uppdaterade?	Ja
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja

3.2.2 Syfte

Genom styrdokument visar PUA att den bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. I styrdokumenten framgår vad som förväntas av medarbetarna när det gäller personuppgiftshantering. Det finns tydliga rutiner för att leva upp till dataskyddsförordningens krav.

3.2.3 Resultat

DSO kontrollerar årligen att grundläggande styrdokument finns upprättade och beslutade/antagna. Det är tydligt vem som är ägare och ansvarig för dokumentationen. Även informationssäkerhetssamordnaren är involverad i arbetet med styrdokumenten.

Bolaget har styrande dokument på plats. Det finns rutiner för personuppgiftsincidenter och konsekvensbedömningar.
De styrande dokumenten håller i huvudsak önskvärd kvalitet. En vidareutveckling kan vara att länken i de anställdas e-postsignatur lydande *”All e-post som skickas till SGA Fastigheter AB kommer att behandlas enligt upprättat dokument ”dataskyddsinformation för SGA Fastigheter” som återfinns på vår hemsida www.sgafastigheter.se”* pekas direkt till den relevanta informationen istället för till hemsidans startsida.

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

3.2.5 DSO ger råd och rekommendationer till PUA

DSO vill påpeka att det följer av gällande lagstiftning att det sker löpande översyn av styrdokumenten. Därför är det av fortsatt vikt att alla chefer får i uppdrag att tillse att dokumentägare till styrdokument genomför detta. DSO och informationssäkerhetssamordnare är behjälpliga och ett stöd för dokumentägarna.

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?	18
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 Syfte

Under 2024 har bolaget, med stöd av SKR:s verktyg KLASSA, informationsklassat 18 stycken fastighetstekniska IT-system. Den senaste klassningen gjordes i december 2024.

3.3.3 Resultat

I systemen finns inga känsliga eller integritetskänsliga personuppgifter. Där finns personuppgifter i form av inloggningsrelaterade uppgifter, såsom namn, e-postadress och telefonnummer till användarna.

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

Personuppgifterna i bolagets system anses inte känsliga enligt dataskyddsförordningen och därmed uppstår inga direkta risker.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Ja, men det finns inga.
Har alla potentiella högriskbehandlingar konsekvensbedömts?	N/A
Är de genomförda bedömningarna aktuella?	Ja

3.4.2 Syfte

Konsekvensbedömningen hjälper bolaget att identifiera och minimera integritetsriskerna för personuppgifter som behandlas. Kravet på konsekvensbedömning följer av dataskyddsförordningen och ska utföras för alla *nya* behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter”.

3.4.3 Resultat

Bolaget har gjort en översyn av att alla behandlingar och genomförda konsekvensbedömningar är aktuella.

Bolaget har inga högriskbehandlingar av personuppgifter.

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

3.4.4 DSO ger råd och rekommendationer till PUA

DSO påminner om att alla chefer löpande ska kontrollera behovet av konsekvensbedömning.

3.5 Individens rättigheter

3.5.1 Sammanfattning

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

3.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen rättigheter som på olika sätt ska garantera att den registrerade personen har insyn i hur dennes personuppgifter hanteras samt har en viss kontroll över personuppgiftsbehandlingen. DSO granskar efterlevnad, identifierar eventuella brister och ger råd för att se till att bolaget har goda rutiner.

3.5.3 Resultat

Ingen har inkommit till bolaget.
Bolaget bedöms ha förutsättningar att hantera registrerades rättigheter inom föreskriven tid.

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 konstaterar att gällande rutiner fungerar tillfredsställande. Det är viktigt att handläggarna är medvetna om vikten av att begäran hanteras inom föreskriven tid (30 dagar).

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Inga incidenter
Hur många personuppgiftsincidenter har dokumenterats?	N/A
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

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland dataskyddsförordningens olika verktyg för att åstadkomma en sund personuppgiftshantering.

3.6.3 Resultat

Inga personuppgiftsincidenter har rapporterats till Integritetsskyddsmyndigheten, IMY.

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 konstaterar att det finns rutiner för incidenthantering och eventuell anmälan till Integritetsskyddsmyndigheten. Dessa har ännu inte prövats.

4 Genomförda granskningar under året

4.1.1 Sammanfattning

Genomförda granskningar:

Det har skett en löpande granskning av bolagets personuppgiftshantering:

- Passerkortslistor
- Behörighetsrevisioner (IT-system)
- Översyn av artikel-30-registret (registerförteckningen)
- Översyn av rutiner och styrdokument

4.1.2 Syfte

En av DSO:s viktigaste uppgifter är att granska hur dataskyddsförordningen efterlevs.

4.1.3 Genomförda granskningar och deras resultat

Organisationen har under året genomfört granskningar som DSO, genom samtal/intervju, fått ta del av granskningens resultat. Nedan redogörs det för i korthet kring granskningarna.

Granskning 1

En granskning av passerkortslistor för behörigheter har genomförts. Vissa personuppgifter krävs, men bolaget är noga med att inga känsliga personuppgifter används i systemen. Löpande gallring sker, så inga inaktuella uppgifter sparas längre än nödvändigt. Det är bolagets hyresgäst som de facto som ansvarar för att uppdatera passerkortssystemet och vilka som är behöriga. Behandlingen utförs dock på uppdrag av bolaget. PUB-avtal finns.

	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

Granskning 2

En granskning av behörigheter till bolagets fastighetstekniska IT-system har genomförts. Vissa personuppgifter krävs, men bolaget är noga med att inga känsliga personuppgifter behandlas. Löpande gallring sker i enlighet med stadens gallringsrutiner, så att inga inaktuella uppgifter sparas längre än nödvändigt.

	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

Granskning 3

Bolaget har genomfört en översyn av sitt artikel-30-register. Vissa förändringar av upplägget har föreslagits för att förenkla och förtydliga dispositionen. Bolaget kommer att arbeta med att implementera förslagen under 2025.

	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

Granskning 4

Det nya, externa DSO har genomfört en översyn av rutiner och styrdokument kopplade till GDPR och informationssäkerhet i samband med att sitt tillträdde under 2024.

	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

DSO ger råd och rekommendationer till PUA

DSO påminner fortsatt om vikten av att hantera känsliga personuppgifter enligt GDPR, såsom sjukdom, på ett korrekt sätt. Detsamma gäller så kallade integritetskänsliga uppgifter, som till exempel personnummer. Detta påtalas löpande och vid behov, direkt till handläggaren eller avsändare av e-post och andra digitala meddelanden. DSO påminner även om löpande gallring av inaktuella och överflödiga personuppgifter, i enlighet med stadens gallringsregler, så att bolaget inte behandlar dessa uppgifter längre än vad syftet kräver.

5 Risker inom dataskydd

5.1.1 Sammanfattning

Relevanta risker inom verksamheten utifrån GDPR:

DSO anser att det i dagsläget inte finns några större risker ur ett *personuppgiftshanteringsperspektiv*, främst utifrån den begränsade mängd personuppgifter som behandlas inom bolaget.

Någon bedömning av dataskyddsaspekter utöver detta har ej genomförts av DSO.

5.1.2 Syfte

Verksamheten ansvarar för att göra vissa typer av riskanalyser, såsom konsekvensbedömningar och informationsklassningar. DSO väljer ut eventuella områden med risker.

5.1.3 Resultatet av riskkartläggningen

DSO har inte gjort någon mer omfattande riskkartläggning då antalet personuppgiftsbehandlingar är få. Den bedömning som kan göras utifrån en generell översyn av verksamheten är att riskerna är små.

	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

5.1.4 DSO ger råd och rekommendationer till PUA

DSO påminner om att dataskyddslagstiftningen kräver en löpande uppföljning av personuppgiftshanteringen. DSO och informationssäkerhetssamordnare är behjälpliga.
Uppstår eller upptäcks brister i bolagets hantering kommer DSO att komma med råd och rekommendationer.

6 Planerade granskningar under det nya verksamhetsåret

6.1.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

Löpande granskning av bolagets personuppgiftshantering:

- Passerkortslistor och behörigheter
- Behörighetsrevisioner
- Artikel-30-registret
- PuB-avtal

6.1.2 Syfte

En planering för granskningar under kommande verksamhetsårets ska göras för att minimera riskerna för felaktig hantering av personuppgifter. Styrt utifrån antalet personuppgiftsbehandlingar kommer granskningar att genomföras löpande och mer omfattande granskningar planeras in om behov uppstår.

7 Övrigt att rapportera

7.1.1 Sammanfattning

Bolaget har få personuppgiftsbehandlingar. Dessa ska givetvis ändå hanteras på korrekt sätt enligt dataskyddsförordningen. Även antalet medarbetare som behandlar känsliga eller integritetskänsliga personuppgifter är mycket begränsat, vilket minskar riskerna för de registrerade. Bolaget har börjat använda digital signering i stor utsträckning, vilket kräver behandling av personnummer från även externa användare. Det finns en rutin för behandlingen av dessa personuppgifter, som också sker inom ramen för av stadens betrodda system för digital signatur.