Stockholms stad

GDPR Årsrapport

2021

SGA Fastigheter AB

GDPR årsrapport
Januari 2021

Dnr: SGAF 2021/19
Utgivningsdatum: 2021-05-03
Kontaktperson: Sara Wallin

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 har relativt få personuppgifter, främst egen personal samt inloggningsuppgifter (som inte anses känsliga).

En registerförteckning skapades inför att dataskyddsförordningen trädde i kraft i maj 2018. Denna uppdateras löpande och vid behov.

Det finns inga direkta brister i hantering eller rutiner. Det har vid några tillfällen under detta pandemiår påtalats för medarbetare att sjukdom är en känslig personuppgift och uppgiften ska därför helst inte skickas med e-post eller annan typ av meddelande. Detta har omgående hanterats med berörd medarbetare.

Denna rapport innehåller ingen sekretessklassad information.

Rapporten är något för omfattande för ett litet bolag som SGA Fastigheter. Vi hade gärna hade sett att det funnit en kortare/komprimerad variant för de mindre verksamheterna inom staden. Risken blir att vi missar de viktiga delarna när det blir en så pass omfattande 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 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?	39
Har nödvändiga uppdateringar gjorts?	Ja
Bedöms registerförteckningen vara fullständig?	Ja
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

Bolaget har en registerförteckning enligt dataskyddsförordningens artikel 30, där samtidiga personuppgiftshanteringar finns dokumenterade. Den uppdateras löpande vid behov, t.ex. systembyte.

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 registerfört 39 behandlingar (verksamhetsprocesser). Det bedöms inte finnas några ytterligare behandlingar som behöver registerföras.

Uppdateringar görs löpande, vid t.ex. systembyte. I bolagets lönesystem finns personuppgifter, även känsliga. I övrigt är det 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 viktigt att bolaget fortsätter att löpande följa upp personuppgiftshanteringen samt att registerförteckningen uppdateras löpande.

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. Det är tydligt vem som är ägare och ansvarig för dokumentationen.
Även informationssäkerhetssamordnaren är involverad i arbetet.

Bolaget har styrande dokument på plats. Det finns rutiner för personuppgiftsincidenter och konsekvensbedömningar.
De styrande dokumenten håller önskvärd 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
	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 anser det viktigt att alla chefer får i uppdrag tillse att alla dokumentägare gör löpande översyn av dokumenten. 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?	En
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 Syfte

Inför införandet av ett nytt fastighetssystem (Pondus Pro) gjordes en informationssäkerhetsklassning med stöd av SKR:s verktyg KLASSA. Detta styr även val och hantering av servrar hos IT-leverantören Tieto.

3.3.3 Resultat

I fastighetssystemet finns inga känsliga 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, 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 är ett krav enligt dataskyddsförordningen och ska utföras för alla behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter”.

3.4.3 Resultat

Bolaget har gjort en konsekvensbedömning av alla behandlingar och genomförda bedömningar är aktuella.
Bolaget har inga högriskbehandlingar av personuppgifter.
Samtliga konsekvensbedömningar är 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
	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 föreslår att alla chefer löpande kontrollerar 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?	En begäran (personen fanns inte i våra register)
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	En

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

Endast en begäran har inkommit till bolaget. Det fanns inga uppgifter om den efterfrågande hos bolaget och hanteringen var betydligt skyndsammare än de 30 dagar som dataskyddsförordningen kräver.

Bolaget har 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 påminna handläggarna 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 Sammanfattning

Genomförda granskningar:

- Det sker en löpande granskning av bolagets personuppgiftshantering.
- Digitala meddelanden med direkt återkoppling till berörda

4.2 Syfte

En av DSO:s viktigaste uppgifter är att granska hur dataskyddsförordningen efterlevs. Detta arbete bedrivs löpande.

4.3 Genomförda granskningar och deras resultat

Granskning 1

Det sker en löpande granskning av bolagets personuppgiftshantering. Då verksamheten är relativt liten är det lättare för DSO att ha insyn i olika delar.

	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

Digitala meddelanden med direkt återkoppling till berörda.
DSO påtalar eventuella brister eller personuppgiftsbehandling i meddelanden som både skickas och tas emot av bolagets medarbetare och entreprenörer. Det kan vara såväl e-post som sms och andra digitala meddelanden. Vid brister påtalas detta omgående till berörda. Bolaget undviker att skicka personuppgifter såsom personnummer, även om dessa inte är känsliga enligt förordningen.

	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

4.4 DSO ger råd och rekommendationer till PUA

DSO påminner om vikten av att hantera känsliga personuppgifter, såsom sjukdom, på ett korrekt sätt. Under pandemin har detta påtalats löpande och vid behov, direkt till handläggaren eller avsändare av e-post och andra digitala meddelanden. Det har även påtalats vid gemensamma möten.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:
DSO anser att det i dagsläget inte finns några större risker, främst kopplat till den lilla mängden personuppgifter som behandlas inom bolaget.

5.2 Syfte

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

5.3 Resultatet av riskkartläggningen

DSO har inte gjort någon mer omfattande riskkartläggning då antalet personuppgiftsbehandlingar är få. Inga risker har upptäckts utan endast mindre brister som omgående rättats till.
Det finns heller ingen direkt risk att personuppgifter delges till fel person/part eller hanteras på annat felaktigt sätt.

	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

5.4 DSO ger råd och rekommendationer till PUA

DSO föreslår en fortsatt löpande uppföljning av personuppgiftshanteringen. DSO och informationssäkerhetssamordnare är behjälpliga.
Uppstår brister i bolagets hantering kommer DSO att komma med råd och rekommendationer.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Löpande granskning av bolagets personuppgiftshantering.
- Digitala meddelanden med icke nödvändiga personuppgifter

6.2 Syfte

En planering för granskningar under kommande verksamhetsårets ska göras för att underlätta DSO:s arbete. Styrt utifrån antalet personuppgiftsbehandlingar kommer granskningar att genomföras löpande och mer omfattande granskningar planeras in om behov uppstår.

7 Övrigt att rapportera

7.1 Sammanfattning

Bolaget har få personuppgiftsbehandlingar. Dessa ska givetvis hanteras på korrekt sätt enligt dataskyddsförordningen. Antalet medarbetare som behandlar känsliga personuppgifter är begränsat och det minimerar riskerna för felbehandling. Dessa behandlingar, såsom hantering av personalens personuppgifter, har även under tidigare lagstiftning behandlats korrekt.