Stockholms stad

# GDPR Årsrapport

2021

Familjebostäder

**GDPR årsrapport**
Januari 2022

**Dnr:** 2021/1437- 2.8.3
**Utgivningsdatum:** 2022-02-22
**Kontaktperson:** Helena Gräntz, Dataskyddsombud

# 1 Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen är att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadgar 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). Dataskyddsombudet 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 dataskyddsombudet är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad dataskyddsombudets 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.

Årsrapporten följer stadsledningskontorets upprättade mall vilken är densamma för Stockholms stads samtliga nämnder och bolag.

De obligatoriska rapporteringsområdena i denna rapport är:

- Registerförteckning
- Styrdokument
- Tekniska och organisatoriska åtgärder för Personuppgiftsbehandlingar
- Konsekvensbedömningar
- Individens rättigheter
- Personuppgiftsincidenter

Inga allvarliga brister i ovanstående områden har identifierats, men det finns förbättringsområden och dessa bör åtgärdas.

Under 2021 har följande granskningar genomförts:

- Fast2 – förekomsten av känslig information
- Fast2 – personuppgiftsbiträdesavtal (granskningen pågår och utförs av extern konsult)
- Kamerabevakning – uppföljning av tidigare identifierade brister

Inte heller här har några allvarlig brister hittills identifierats, men det finns förbättringsområden och dessa bör åtgärdas.

I denna rapport framgår vidare vilka risker bolaget utifrån dataskyddsförordningens krav:

- Hantering av hyresgäster med skyddad identitet i Fast2
- Systematiskt dataskyddsarbete
- Kamerabevakning och låssystem
- Tredjelandsöverföringar

Riskerna är kända av verksamheten och det arbetas för att minimera dessa på olika sätt och dataskyddsombudet stöttar upp i detta arbete.

Även om det finns förbättringsområden för att öka bolagets efterlevnad till dataskyddsförordningen, så finns det kunskap och vilja att göra rätt vilket innebär att förutsättningarna för det fortsatta utvecklingsarbetet är goda.

# 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
- Personuppgiftsincidenter

Nedan redogörs för bolagets status och dataskyddsombudets slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter genomförda uppföljning och granskning.

## 3.1 Registerförteckning

### 3.1.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Antal behandlingar som är registrerade? | 182 |
| Har nödvändiga uppdateringar gjorts? | Delvis |
| Bedöms registerförteckningen vara fullständig? | Delvis |
| Har verksamheten lämpliga rutiner för registerföring? | Nej |

### 3.1.2 Syfte

En registerförteckning är ett krav enligt dataskyddsförordningen. (Artikel 30). För att något ska gå att skydda måste det först vara synligt för verksamheten. Alla processer i bolaget ska kartläggas i syfte att identifiera aktuella personuppgiftsbehandlingar. Dessa ska sedan registreras i bolagets registerförteckning.

Registerförteckningen är dataskyddsarbetets centrala utgångspunkt och bas samt säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling.

Med kravet på dokumentation uppfyllt kan verksamheten arbeta effektivt, systematiskt och riskbaserat och samtidigt värna individens integritet, särskilt när känsliga och särskilt skyddsvärda personuppgifter behandlas.

### 3.1.3 Resultat

Arbetet med inventering av personuppgifter och upprättande av registerförteckning påbörjades våren 2018. Registerförteckningen består av flera delar som, förutom att säkerställa en laglig grund för behandlingen, ska se till att verksamheten tar ställning till behov av konsekvensbedömning och att uppgifter skyddas på ett ändamålsenligt sätt.

Familjebostäders registerförteckning är omfattande och innehåller de mest väsentliga personuppgiftsbehandlingarna. Under 2021 har delar av registerförteckningen uppdaterats dels med nya behandlingar, dels för att passa in i Stockholms stads mall, som nyligen har uppdaterats.

Ett identifierat utvecklings- och förbättringsområde kopplat till registerförteckningen är att bolaget saknar tillräckliga rutiner som säkerställer att nya personuppgiftsbehandlingar registreras i registerförteckningen.

*Antal registrerade behandlingar?*
182

*Har nödvändiga uppdateringar gjorts?*
Delvis, men det finns behov av att säkerställa att nya behandlingar registreras i systemet samt att befintliga behandlingar förs in i den uppdaterade mallen.

*Bedöms registerförteckningen vara fullständig?*
I registerförteckningen finns de mest väsentliga kända behandlingar av personuppgifter identifierade. Samtliga behandlingar har stöd i lag.

Varje behandling ska därefter bedömas i olika steg. De återstår att dokumentera ställningstaganden och beslut för flera av behandlingarna till exempel gällande lagringstid.

*Har bolaget tillräckliga rutiner för registerföring?*
Bolagets dataskyddsgrupp, som består att sju utsedda dataskyddssamordnare samt dataskyddsombudet, träffas cirka två gånger per halvår för att diskutera dataskyddsfrågor. Nya personuppgiftsbehandlingar och gällande rutiner tas upp regelbundet.

Det finns behov av att ta fram rutiner inom avdelningar/enheter för att säkerställa att nya personuppgiftsbehandlingar registreras i registerförteckningen.

### 3.1.4 Dataskyddsombudet 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 Dataskyddsombudet ger råd och rekommendationer till PUA

Processer som behandlar känsliga personuppgifter har prioriterats i dataskyddsarbetet och det är säkerställt att ansvaret uppfylls. De brister som återstår handlar om kvalitetsförbättringar och uppdateringar.

Systemet Draftit har inbyggda funktioner som säkerställer en hög kvalitet för registerförteckning och ger möjlighet att identifiera risker. Systemet är ett viktigt verktyg för ett systematiskt dataskyddsarbete och bolaget bör fortsätta arbetet med överföring av uppgifter till systemet.

Processägare rekommenderas att ta fram rutiner för att säkerställa att nya personuppgiftsbehandlingar registreras i Draftit. Bolaget behöver inte särskilja varje moment där personuppgifter behandlas, utan kan göra en samlad registrering för en viss process.

Dataskyddsombudet har idag en nyckelroll kopplat till registerförteckningen, vilket inte är förenligt med dataskyddsförordningens krav på oberoende. Förslagsvis bör ansvaret för uppdatering av registerförteckningen ligga hos ansvarig för respektive process alternativt hos någon med ansvar för dataskyddsfrågor på bolaget.

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

### 3.2.2 Syfte

En viktig del i dataskyddsarbetet 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. Genom styrdokument visar PUA att det bedrivs ett systematiskt dataskyddsarbete.

Genom styrdokument kommunicerar PUA till medarbetare i sin verksamhet om vad som gäller och vad som förväntas av medarbetarna. 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.

### 3.2.3 Resultat

*Finns lämplig styrande dokumentation på plats?*
Det finns skriftlig dokumentation som beskriver hur information ges till registrerade och hur registrerades rättigheter tillvaratas.
Det finns rutin och anvisning för hantering av personuppgiftsincidenter.

Det finns anvisning för när och av vem en konsekvensbedömning avseende dataskydd ska genomföras.

Det finns riktlinje för hantering av foton på anställda och andra finns samt mall för samtycke i de fall det är aktuellt.

Rutin för hur verksamheten hanterar inbyggt dataskydd och dataskydd som standard i verksamhetens processer och rutiner kan utvecklas.

Det saknas i huvudsak skriftliga rutiner och anvisningar hos avdelningar/enheter som ska utgöra ett stöd för medarbetarnas dagliga arbete

*Håller innehållet i de existerande dokumenten tillräcklig kvalitet?*
De dokument som finns framtagna är ändamålsenliga och tydliga. Anvisningar för medarbetare som har kundkontakter är till exempel utformade som ”lathund” med konkreta exempel på vanligt förekommande problem och hur de hanteras.

Familjebostäders personuppgiftspolicy uppdaterades under 2020 och finns tillgänglig för såväl medarbetare som kunder.

### 3.2.4 Dataskyddsombudet 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 |

### 3.2.5 Dataskyddsombudet ger råd och rekommendationer till PUA

Identifierade brister har en påverkan på bolagets möjlighet att följa kraven i dataskyddsförordningen och åtgärder bör vidtas.

Genom styrdokument visar PUA att det bedrivs ett systematiskt dataskyddsarbete. Det är dock viktigt att styrdokumenten är kommunicerade och kända för berörda medarbetare.

Processansvariga rekommenderas att säkerställa att det finns dokumenterade och kommunicerade rutiner. Särskilt fokus bör läggas på nyckelpersoner som chefer eller andra ansvariga för att utveckla dataskyddsarbetet och se till att det integreras i verksamhetens processer.

## 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? | Omkring 65-70 procent av Familjebostäders system är klassade i verktyget KLASSA åtminstone en gång. |
| Är klassade personuppgiftsbehandlingar aktuella? | Ja. |

### 3.3.2 Syfte

Personuppgiftsansvarig ska genomföra lämpliga (tekniska) och organisatoriska åtgärder (strategier) för att säkerställa och kunna visa att behandling av personuppgifter utförs i enlighet med förordningen.

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. Genom informationsklassningen har verksamheten förutsättningar att välja rätt åtgärder för att skydda sin information. Organisatoriska åtgärder innebär att det finns styrdokument och rutinbeskrivningar som är kommunicerade och kända i organisationen.

### 3.3.3 Resultat

Informationsklassning har genomförts för merparten av de system där personuppgifter behandlas. Klassningarna är genomförda under det senaste året. Dataskyddsombundet har blivit informerad om de klassningar av systemen som behandlar personuppgifter och har i vissa fall deltagit i klassningen.

Brister som noterats under klassningen handlar om dokumentation av rutiner och anvisningar för systemen, inte i de delar som gäller behandling av personuppgifter.

Granskningen av rapporteringsområdena registerförteckning och konsekvensbedömning visade att rutinerna inte är kända i organisationen.

### 3.3.4 Dataskyddsombudet 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 |

### 3.3.5 Dataskyddsombudet ger råd och rekommendationer till PUA

Styrdokument och rutiner som rör dataskydd bör lyftas och göras mer kända. Särskilt fokus bör läggas på chefer och ansvariga för processer, för att säkerställa att dataskyddsarbetet integreras i verksamhetens processer.

## 3.4 Konsekvensbedömningar

### 3.4.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av? | Delvis |
| Har alla potentiella högriskbehandlingar konsekvensbedömts? | Inga högriskbehandlingar har identifierats |
| Är de genomförda bedömningarna aktuella? | Ja |

### 3.4.2 Syfte

Konsekvensbedömningen anses liksom registerförteckning och informationsklassning som ett viktigt verktyg för verksamhetens dataskyddsarbete.

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. Konsekvensbedömning ska utföras för alla behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter”. Baserat på bedömningen kan/ska riskförebyggande åtgärder vidtas.

### 3.4.3 Resultat

Det har bedömts och noterats i registerförteckningen att ingen behandling innebär en ”sannolikt hög risk för fysiska personers rättigheter och friheter”. Det finns en dokumenterad riskanalys för besluten för noteringen.

En personuppgiftsansvarig måste kunna visa att dataskyddsförordningens principer för behandling av personuppgifter efterlevs och därav är dokumenterade underlag en styrka.

En identifierad svaghet är att behovet av konsekvensbedömning uppmärksammas i sent skede vid upphandling

### 3.4.4 Dataskyddsombudet 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 Dataskyddsombudet ger råd och rekommendationer till PUA

Konsekvensbedömning är ett område som bolaget har anvisningar och rutiner för. De är kommunicerade, men behöver implementeras i processer för att blir kända samt integrerade i verksamhetens dataskyddsarbete.

## 3.5 Individens rättigheter

### 3.5.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer? | 1 |
| Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar? | 1 |

### 3.5.2 Syfte

Registrerade personer har ett antal rättigheter som på olika sätt ska garantera att den registrerade har insyn i hur dennes personuppgifter hanteras samt har en viss kontroll över personuppgiftsbehandlingen. Det är ett krav enligt förordningen att personuppgiftsansvarig tillgodoser rättigheterna.

Rättigheterna medför en rätt att ställa krav, som exempelvis att få ett så kallat registerutdrag eller att få uppgifter rättade. Rätten till radering, den så kallade ”rätten att bli glömd”, är sällan aktuell, eftersom stadens verksamheter lyder under krav på bevarande till följd av offentlighetsprincipen.

Verksamheten har en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran. Att leva upp till förordningens tidskrav på 30 dagar är mycket viktigt för att upprätthålla allmänhetens förtroende för hur staden hanterar personuppgifter.

### 3.5.3 Resultat

Familjebostäder har tagit emot en begäran om registerutdrag. Begäran inkom 2021-11-10, personen fick svar 13 dagar senare. Under 2020 inkom totalt tre begäran om registerutdrag.

Det finns en ett strukturerat arbetssätt kopplat till begäran av registerutdrag, men i merparten av våra system kräver manuell hantering för att ta fram uppgifter om en person. Manuell hantering innebär typiskt sett en risk för fel och betraktas vanligtvis som en risk.

### 3.5.4 Dataskyddsombudet 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 Personuppgiftsincidenter

### 3.6.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Hur upptäcks personuppgiftsincidenter? | Medarbetare (kundservice fastighetsavdelningen, digital utveckling), via leverantörer eller via Stockholm stad |
| Hur många personuppgiftsincidenter har dokumenterats? | 10 |
| Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte? | 2 |
| Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten? | 1 |

### 3.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskydds-förordningen ”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 viktigt och obligatoriskt enligt dataskyddsförordning. Incidenthanteringen består av två huvudsakliga moment – rapportering respektive dokumentation.

*Rapporteringsskyldighet*
Rapporteringsskyldighet gäller som huvudregel. Undantag från rapporteringsskyldigheten gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter”

Bristande förmåga att rapportera personuppgiftsincidenter i tid kan leda till sanktioner.

*Dokumentationskrav*
Alla personuppgiftsincidenter ska dokumenteras, även i de fall då incidenten inte ska rapporteras till IMY. Bristande dokumentering strider mot dataskyddsförordningen. Omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits ska dokumenteras. Bristande dokumentering är sanktionsgrundande.

### 3.6.3 Resultat

Dokumentationskravet har uppfyllts, men inte rapporterings-skyldigheten till IMY. I ett fall fick dataskyddsombudet information om incidenten fem dagar efter att incidenten identifierats, vilket innebär att rapporteringskravet till IMY inte kunde uppfyllas. Efter en tids utredning framkom dock att incidenten inte var allvarlig.

Alla incidenter som blir kända hanteras och dokumenteras av dataskyddsombudet, viktigare händelser rapporteras till vd. En incident har under 2021 rapporterats till IMY. Incidenten registrerades med lägsta risknivå efter att utredningen var klar.

Personuppgiftsincidenthantering följer samma rutin som övrig incidenthantering inom bolaget. Bolaget har hanterat situationer då incident inledningsvis bedömts behöva rapporteras, men utredningen visat att det inte behövts.

Medarbetare får information om vad en personuppgift är samt hur sådana ska anmälas. Rutinen för incidentrapportering finns även tillgängligt på intranätet. Dock finns det med största sannolikhet ett mörkertal incidenter och då särskilt för de som klassas som mindre allvarliga.

En vanlig personuppgiftsincident är att e-post skickas till fel person utanför bolaget. Det har också uppdagats att känslig information[1] noteras i fritextfält i bolagets fastighetssystem. Detta har dock inte registrerats som en incident, men det är en brist avseende efterlevnaden till dataskyddsförordningen.

[1] Känslig information i det här sammanhanget är uppgift om en persons hälsotillstånd, att personen till exempel är döv är sjuk eller ligger på sjukhus.

### 3.6.4 Dataskyddsombudet 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 Dataskyddsombudet ger råd och rekommendationer till PUA

Risken med att inte hantera incidenter på ett tillförlitligt sätt är att bolaget inte lever till dataskyddsförordningens krav, vilket kan föranleda såväl vite från tillsynsmyndigheten som bristande förtroende från intressenter som kunder och leverantörer.

Personuppgiftsansvarig rekommenderas att tillförsäkra sig om att anställda känner till gällande rutiner för att minska risken för att personuppgiftsincidenter inte hanteras på ett korrekt sätt.

Personuppgiftsansvarig rekommenderas vidare att ta fram rutiner för hur anställda får uttrycka sig i fastighetssystemet Fast2. Familjebostäder har inte en laglig grund för att hantera uppgifter kopplat till kundernas hälsa.

# 4 Genomförda granskningar under året

## 4.1 Sammanfattning

Genomförda granskningar under 2021:

- Fast2 – förekomsten av känslig information
- Fast2 – personuppgiftsbiträdesavtal (granskningen utförs av extern konsult)
- Kamerabevakning – uppföljning av tidigare identifierade brister

## 4.2 Syfte

En av dataskyddsombudet 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

*Förekomsten av känslig information i Fast2*

I Fast2 har vi all information om våra hyresgäster. Den lagliga grunden till denna/dessa behandlingar är hyresavtalet.

Mot bakgrund av att vi har en avtalssituation med hyresgästerna får vi hantera personuppgifter som exempelvis namn, adress, kontaktuppgifter och avtalsnummer. Vi har dock ingen laglig grund för att hantera känslig information som uppgifter om hälsa om våra hyresgäster.

| | |
|---|---|
| | 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 |

*Fast2 – granskning av personuppgiftsbiträdesavtal*

Granskningen pågår och utförs av externa konsulter. Resultatet kommer att redovisas under första kvartalet 2022.

*Kamerabevakning – uppföljning av tidigare identifierade brister*

Under 2019 genomförde dataskyddsombudet en granskning av bolagets rutiner gällande kamerabevakning. Kamerabevakning är en integritetskänslig personuppgiftsbehandling varför det krävs andra åtgärder innan en kamera får sättas upp.

Inför en kamerabevakning är det viktigt att vi dokumenterar våra bedömningar samt säkerställa att principerna om uppgiftsminimering, lagringsminimering och säkerhet för uppgifterna beaktas.

Slutligen är den som ska kamerabevaka skyldig att informera om att en plats är kamerabevakad. En sådan upplysning ska lämnas genom tydlig skyltning eller på annat verksamt sätt.

| | |
|---|---|
| | 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 |

# 5 Risker inom dataskydd

## 5.1 Sammanfattning

Relevanta risker inom verksamheten:

- Hantering av hyresgäster med skyddad identitet i Fast2
- Systematiskt dataskyddsarbete
- Kamerabevakning och låssystem
- Tredjelandsöverföringar

## 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. För att bedöma risker genomför dataskyddsombudet en egen riskkartläggning med stöd av stadens riktlinjer.

De risker som nämns i stycket nedan är kända av verksamheten och det arbetas för att minimera dessa på olika sätt och dataskyddsombudet stöttar upp i detta arbete.

## 5.3 Resultatet av riskkartläggningen

*Hantering av hyresgäster med skyddad identitet i Fast2*

| | |
|---|---|
| | 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 |

*Systematiskt dataskyddsarbete*

| | |
|---|---|
| | 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 |

*Kamerabevakning*

| | |
|---|---|
| | 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 |

*Tredjelandsöverföringar*

| | |
|---|---|
| | 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 |

## 5.4 Dataskyddsombudet ger råd och rekommendationer till PUA

*Hantering av hyresgäster med skyddad identitet i Fast2*
En översyn av hur bolaget registrerar hyresgäster med skyddad identitet i Fast2 visar att samtliga medarbetare som har behörighet till systemet får vetskap om hyresgästen är skyddad eftersom hyresgästens namn benämns ”uppges ej”. Bolaget har även haft incidenter där hyresgäster med skyddad identitet exponerats som ”uppges ej” också i trapphus. Det har genomförts en översyn av hur hyresgäster med skyddad identitet ska hanteras och aktuella verksamheter arbetar för att hitta en ändamålsenlig lösning.

Dataskyddsombudet rekommenderar att det skapas en mer ändamålsenlig och säker hantering av personuppgifter kopplat till hyresgäster med skyddad identitet.

*Systematiskt dataskyddsarbete*
Förutsättningar för ett ändamålsenligt dataskyddsarbete är att roller och ansvar är dokumenterat, kommunicerat och väl etablerat i organisationen.

Dataskyddsarbetet är inte i alla delar etablerat i hela organisationen. Brister visar sig bland annat i att dataskyddsombudet i ett sent skede blir involverad i dataskyddsdiskussioner som till exempel konsekvensanalyser.

Det finns behov att ta ett samlat/övergripande grepp om bolagets dataskyddsarbete och skapa ökad kunskap om att verksamheten ansvarar för att det finns dokumenterade rutiner kopplat till dataskydd.

Dataskyddsombudet rekommenderar att en GAP-analys/översikt över organisationens GDPR-efterlevnad tas fram.

*Kamerabevakning och elektroniska låssystem*
Att utföra kamerabevakning inskränker på den enskildes integritet. Den som bedriver bevakning är ansvarig för att nödvändiga bedömningar har genomförts för att säkerställa att behandlingen är laglig.

Likt kamerabevakning innebär låssystemet risker för den enskildes integritet om informationen i systemet används på ett felaktigt sätt. En stinggent behörighetsstyrning samt kunskap om hur information i systemet får hanteras är väsentliga åtgärder för att minska risken för felaktig användning av personuppgifter.

Utmaningen med personuppgiftshanteringen vid kamerabevakning samt elektroniska låssystem är kända inom berörda verksamheter och arbete pågår för att minimera de kända riskerna.

Dataskyddsombudet rekommenderar att:
- Befintlig kamerabevakning utvärderas för att säkerställa att det finns underlag som styrker behovet av övervakning.
- Roller och ansvar förtydligas avseende låssystemet Aptus samt att rutiner för att trygga en säker användning av systemet tas fram.

*Tredjelandsöverföringar*
Överföring av personuppgifter till ett land utanför EU/EES (tredjeland) kräver särskilt tillstånd.

Dataskyddsombudet rekommenderar att bolaget slutför kartläggningen över vilka avtalssituationer det finns risk för att personuppgifter kan överföras till tredjeland för att i ett nästa steg bedöma om de eventuella överföringarna är lagliga. Därtill behöver behovet av personuppgiftsbiträdesavtal ses över.

# 6 Planerade granskningar under det nya verksamhetsåret

## 6.1 Sammanfattning
Relevanta granskningsområden inom verksamheten:
- Rutiner och kontroller för behörigheter
- Uppföljning av rutiner för kamerabevakning och digitala låssystem

## 6.2 Syfte

Som nämnts ovan är det granskande arbetet en av dataskyddsombudets viktigaste uppgifter. Granskningsområdena väljs med fokus på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister.

## 6.3 Planerade granskningar

### *Rutiner och kontroller för behörigheter (grundläggande principer, artikel 5)*

Personuppgiftsansvarig måste se till att personuppgifterna skyddas på ett bra sätt genom att vidta lämpliga säkerhetsåtgärder. Alla personuppgifter som behandlas måste skyddas, så att ingen obehörig kommer åt dem och så att de inte används på ett otillåtet sätt.

Dataskyddsombudet planerar att i samverkan med bolagets informationssäkerhetssamordnare se över styrning och kontroll av behörighetstildelning.

### *Uppföljning av rutiner för kamerabevakning och digitala låssystem*

Dataskyddsförordningen gäller vid varaktig eller regelbundet upprepad personbevakning eftersom det innebär en personuppgiftsbehandling. Personbevakning är bevakning där människor utan större svårigheter kan identifieras.

För att säkerställa att kamerabevakningen är tillåten finns det bestämmelser i dataskyddsförordningen som måste vara uppfyllda. Även digitala låssystem innebär behandling av personuppgifter som sker i nära anslutning till den privata sfären, det vill säga bostaden. Med tanke på detta finns anledning att i särskilt hög grad beakta de boendes integritetsintresse.

Dataskyddsombudet planerar att se över ansvar, roller och rutiner för kamerabevakning samt digitala låssystem för att säkerställa att bolaget lever till upp aktuella krav i dataskyddsförordningen.

# 7 Övrigt att rapportera

Dataskyddsombudet uppmärksammar händelser, rapporterar och ger information och råd löpande under året. Varje månad skickas ett månadsbrev ut till utsedda dataskyssamordnare och andra nyckelpersoner i bolaget. Därtill hålls separata möten med

dataskyddssamordnarna och under 2021 och tre sådana ägt rum. Frågor från verksamheten besvaras löpande till följd av rekommendationer som syftar till att öka dataskyddet.

I samråd med informationssäkerhetssamordnaren har en checklista som ska fyllas i inför införandet av nya system arbetats fram. En likvärdig checklista finna även framtagen anpassad till upphandlingsprocessen. Checklistorna innehåller även frågor avseende tredjelandsöverföringar, som är en aktuell fråga med anledning av den tidigare Schrems II-domen.

Arbetet med att kartlägga bolagets eventuella tredjelands-överföringar hanteras av enheten för digital utveckling och dataskyddsombudet har under året haft kontinuerliga dialoger med bland annat aktuell gruppchef. Kartläggningsarbetet pågår men det saknas en fulltäckande bild över tredjelandsöverföringar. Likaså gäller behovet av personuppgiftsbiträdesavtal för befintliga avtal, men även det arbetet pågår.

Dataskyddsombudet har under året haft en nära samverkan med dataskyddsombuden på de andra kommunala bostadsbolagen (Svenska Bostäder, Stockholmshem och Micasa). Samarbetet har bland annat mynnat ut i den gemensamma granskningen av Fast2 följsamhet till upprättat personuppgiftsbiträdesavtal. I övrigt har det skett samverkan avseende hantering av hyresgäster med skyddad identitet i Fast2.