Stockholms stad

Dataskyddsombudets årsrapport

Januari 2023

Micasa Fastigheter

Dataskyddsombudets årsrapport
Januari 2023

Dnr: MIC 2023/8
Utgivningsdatum: 2022-01-03
Kontaktperson: Anne Tawstman

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. För 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

1 Bakgrund 3

2 Sammanfattning 5

3 Obligatoriska rapporteringsområden 6

3.1 Registerförteckning 6

3.2 Styrdokument 9

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar 11

3.4 Konsekvensbedömningar 13

3.5 Individens rättigheter 14

3.6 Personuppgiftsincidenter 16

4 Genomförda granskningar under året 18

4.1 Sammanfattning 18

4.2 Syfte 18

4.3 Genomförda granskningar och deras resultat 18

4.4 DSO ger råd och rekommendationer till PUA 19

5 Risker inom dataskydd 20

5.1 Syfte 20

5.2 Resultatet av riskkartläggningen 21

5.3 DSO ger råd och rekommendationer till PUA 21

6 Planerade granskningar under det nya verksamhetsåret 22

6.1 Sammanfattning 22

6.2 Syfte 22

6.3 Planerade granskningar 22

7 Övrigt att rapportera 23

7.1 Granskning Fast 2 23

7.2 Dataskyddsgruppen 25

2 Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

Jag vill inleda med att berätta att granskning av fastighetssystemet Fast2 avslutats. Granskningen visade brister i leverantörens dataskyddsarbete, vilket i förlängningen kan innebära risker för bolaget. Krav på åtgärder har ställts på Fast2 och en förnyad granskning ska genomföras, för att följa upp att åtgärderna genomförts.

DSOs uppdrag är bland annat att granska hur väl organisationen uppfyller dataskyddsförordningens krav och ge råd. Jag upplever att det är lätt att bli lyssnad på som DSO. Organisationen tar till sig information och råd jag ger. Det blev tydligt när resultatet av granskningen av Fast2 redovisades och bolaget följde de rekommendationer som gavs.

Att bolaget känner till var verksamheten har brister, är en viktig del i ett riskbaserat arbetssätt. Det är därför positivt att bolaget under året tecknat avtal för fler tjänster i verktyget Draftit. Systemet har inbyggda funktioner som underlättar ett riskbaserat och systematiskt dataskyddsarbete. Systemet används nu inte bara för registerförteckning utan även för risk- och konsekvensbedömning samt incidentrapportering.

För mig som DSO är det glädjande att rapportera att det hos bolaget finns en medvetenhet för dataskyddsförordningens krav. Jag avslutar årets rapport med att berätta om dataskyddsgruppens arbete som steg för steg förbättrar det systematiska dataskyddsarbetet.

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:s slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:s genomförda uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	22 registreringar *(16 året innan)*
Har nödvändiga uppdateringar gjorts?	Ja
Bedöms registerförteckningen vara fullständig?	Ja, men kvalitetsförbättring behöver fortsätta
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

För att något ska gå att skydda måste det först vara synligt för verksamheten. Alla som behandlar personuppgifter måste inventera personuppgifter som behandlas i verksamheten och dokumenterat dem i en så kallad registerförteckning. En registerförteckning är ett krav enligt dataskyddsförordningen. (Artikel 30)

Micasa Fastigheter har en digital registerförteckning i systemet Draftit. Registerförteckningen är dataskyddsarbetets centrala utgångspunkt och bas, den 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

Registerförteckningen består av flera delar som, förutom att säkerställa en laglig grund för behandlingen, även säkerställer att verksamheten tar ställning till behov av konsekvensbedömning och att uppgifter skyddas på ett ändamålsenligt sätt.

Sedan årsskiftet 2022 har bolaget tecknat avtal för flera tjänster i verktyget Draftit. Förutom registerförteckningen som använts sedan 2020 använder bolaget även Draftit för dokumentation av incidenter och för risk- och konsekvensanalys.

Antal behandlingar som är registrerade?
Bolaget har registrerat sex nya processer i registerförteckningen. Det har skett i samband med att nya system eller program börjat användas.

Har nödvändiga uppdateringar gjorts?
Ja. Registerförteckningen har löpande uppdaterats med nya behandlingar eller efter förändrade processer för behandling av personuppgifter.

Bedöms registerförteckningen vara fullständig?
I registerförteckningen finns alla kända behandlingar av personuppgifter identifierade. Alla behandlingar har stöd i lag.

Varje behandling ska därefter bedömas i olika steg. De återstår fortfarande att dokumentera riskbedömningar, ställningstaganden och beslut för flera av behandlingarna.

Har verksamheten lämpliga rutiner för registerföring?
Ja, lämpliga rutiner finns. Bolagets dataskyddsgrupp består av medarbetare med olika roller i bolaget. Bolaget har ett pågående aktivt dataskyddsarbete. I arbetet ingår även arbete med registerförteckningen.

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

Processer som behandlar känsliga personuppgifter, tex processer som behandlar personalärenden eller hyresgästärenden prioriteras i dataskyddsarbetet, det är säkerställt att ansvaret uppfylls. De brister som återstår handlar om kvalitetsförbättringar.

3.1.5 DSO ger råd och rekommendationer till PUA

Systemet Draftits inbyggda funktioner säkerställer en hög kvalitet för registerförteckning och ger möjlighet att identifiera risker. Systemet är ett viktigt verktyg för ett systematiskt dataskyddsarbete. Bolaget bör fortsätta kvalitetssäkra uppgifterna i systemet.

Arbetet med att tydliggöra ansvaret och att fortsätta utbilda processägare för att säkerställa ett systematiskt dataskyddsarbete, bör fortsätta även under kommande år.

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, men behöver uppdateras
Är dokumenten uppdaterade?	Ja, men behöver uppdateras
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Behöver uppdateras

3.2.2 Syfte

En röd tråd i Dataskyddsförordningen 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.

Dokumenterade rutiner och styrdokument ingår även i det som kallas *organisatoriska åtgärder*.

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?
Det finns skriftliga rutiner och anvisningar för medarbetarnas dagliga arbete, 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 saknas rutin för hur verksamheten hanterar inbyggt dataskydd och dataskydd som standard i verksamhetens processer och rutiner.

Det finns Riktlinjer för publicering av bilder och film på tex bolagets webbsida eller i sociala medier.

Håller innehållet i de existerande dokumenten lämplig kvalitet?
De flesta dokument som finns är ändamålsenliga, lättlästa 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.

Bolaget har en personuppgiftspolicy som tydligt beskriver att Micasa Fastigheter värnar om skyddet av den personliga integriteten.

Det har under åren tillkommit information om arbetssätt och rutiner som publicerats på den interna webbsidan Enok. I takt med att ny information lagts till, har det blivit allt svårare att snabbt hitta relevant information.

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

Behov av uppdatering
Det är positivt att arbetssätt och rutiner tydliggjorts, men det har samtidigt blivit svårare att lätt hitta informationen. Ny information har lagts till och det har blivit svåröverskådligt.

En mer överskådlig och lättillgänglig struktur för hur rutiner, dokument och anvisningar rekommenderas. Samtidigt bör innehållet gås igenom och vid behov uppdateras.

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?	7 genomförda 1 ny påbörjad
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.

3.3.3 Resultat

Bolaget har ett pågående informationssäkerhetsarbete som samordnas med dataskyddsarbetet.

Under året har bolaget anpassat sig till stadens nya riktlinjer för hur handlingsplaner för informationsklassade system sparas. Handlingsplaner sparas nu digitalt i dokument och ärendehanteringssystemet eDok. Det nya arbetssättet innebär ett förbättrat skydd för bolagets analyser och handlingsplaner.

DSO har deltagit i klassningen av systemen som behandlar personuppgifter. Informationsklassning har genomförts för samtliga system där personuppgifter behandlas. Klassningarna är i vissa fall genomförda för några år sedan åren och kommer därför behöva göras om för att vara aktuella.

Brister som noterats under klassningen har handlat om behov av dokumentation av rutiner och anvisningar för systemen.

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

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?	Det pågår bedömning av en potentiell högriskbehandling.
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

Under året har systemet Draftits modul för konsekvensbedömning tagits i bruk. Bedömning och dokumentation sparas nu samlat tillsammans med registerförteckningen.

Fastighetssystemet Fast2 genomgår för närvarande en fullständig konsekvensbedömning.

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

Risk- och konsekvensbedömning av systemet Fast2 bör slutföras.

Därefter bör processer som hanterar känsliga hyresgästfrågor (tex störningar i boendet) bedömas och dokumenteras i systemet Draftit.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	0
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	-

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. (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 30 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

Det saknas ett strukturerat arbetssätt och det krävs manuell hantering för att ta fram ett registerutdrag. Manuell hantering innebär typiskt sett en risk för fel och betraktas vanligtvis som en brist.

Bolaget har förhållandevis få registrerade. Sedan 2018 har endast en begäran från en registrerad hanterats och med god tidsmarginal (inom 3 dagar). I det sammanhanget är bristerna inte av nämnvärd betydelse.

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

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Handläggare i kundtjänst uppmärksammar, genom DSOs kontroller och genom information från staden.
Hur många personuppgiftsincidenter har dokumenterats?	7
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	2 rapporterades till IMY 1 berörd person informerades
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Båda

3.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskyddsförordningen ”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.
(Integritetsskyddsmyndigheten)

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 och rapporteringsskyldigheten uppfylls.

Alla incidenter som blir kända hanteras och dokumenteras i systemet Draftit. Systemet fungerar på så vis att ansvarig chef uppmärksammas på de incidenter som sker.

Incidenthantering följer samma rutin som övrig incidenthantering inom bolaget.

Medarbetare utbildas i att känna igen personuppgiftsincidenter och hur de anmäls.

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

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Den personuppgiftsansvariges ansvar, Artikel 24
- Konsekvensbedömning avseende dataskydd, Artikel 35

4.2 Syfte

En av dataskyddsombudets 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.

Granskningsområdena väljs med focus på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister.

4.3 Genomförda granskningar och deras resultat

Den personuppgiftsansvariges ansvar, Artikel 24

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

Organisatoriska åtgärder handlar om administrativt säkerhetsarbete, där ingår, förutom informationsklassning även interna rutiner och riktlinjer. Granskningsområdet har varit samma under de senaste åren. Anledningen är att tidigare granskningar visat att rutiner inte alltid följs.

DSO gav följande råd i förra årets rapport:

”DSO råder PUA att genomföra utbildning och uppdatera rutiner på de enheter som hanterar känsliga hyresgästuppgifter. DSO råder även PUA att prioritera införande av digitalt stöd för ärendehantering.”

DSO har även under 2022 uppmärksammat brister i följsamhet av rutiner och anvisningar. Känslig information om hyresgäster har sparats på ett sätt som möjliggjort för obehöriga handläggare att få tillgång till informationen. Händelser har registrerats som incidenter. Händelserna har utretts och följts upp tillsammans med ansvarig chef.

Under 2022 har eDok, ett nytt ärende- och dokumenthanteringssystem införts. Ärenden som innehåller känsliga personuppgifter kan nu diarieföras och hanteras digitalt i eDok och sekretess kan läggas så endast behöriga handläggare får tillgång till uppgifterna. eDok är en viktig förbättring som stärker skyddet av personuppgifter.

	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

4.4 DSO ger råd och rekommendationer till PUA

Den personuppgiftsansvariges ansvar, Artikel 24

DSO ger PUA samma råd som under 3.2.5, som handlar om styrdokument. PUA bör se över viktiga arbetssätt och rutiner och vid behov uppdatera dem.

Genom nedtecknade och kommunicerade rutiner och styrdokument blir det tydligt vad som förväntas av medarbetarna.

Konsekvensbedömning avseende dataskydd, Artikel 35

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.

DSOs granskning visar att bolaget genomför risk- och konsekvensbedömningar med stöd av systemet Draftit.

	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 Risker inom dataskydd

5.1 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.

Allvarliga risker som bör prioriteras kan röra till exempel personuppgiftsbehandlingar som innebär höga risker, tredjelandsöverföringar, brister i verksamhetens rutiner, brister i verksamhetens mejlhantering, rutiner kring känsliga personuppgifter mm.

5.2 Resultatet av riskkartläggningen

Organisering och struktur

När bolagets egen personal brister i efterlevnad av rutiner, innebär det en risk för skyddet av personuppgifter. Brister i verksamhetens rutiner betraktas vanligtvis som allvarligt.

Incidenter som DSO uppmärksammat har, även under 2022, handlat om att personuppgifter sparats på ett felaktigt sätt. För registrerade personer har bristerna inte inneburit några personliga konsekvenser.

DSO har noterat att samma misstag upprepats. Det finns därför en risk att bristen på efterlevnad av rutiner leder till förlust av konfidentialitet och förlorat förtroende.

Bolaget har förhållandevis få registrerade personer och medarbetare som behandlar personuppgifter. De uppgifter som behandlas är inte av den mest känsliga karaktären. Sammantaget bedömer DSO att bristerna inte kräver omgående åtgärder.

	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

5.3 DSO ger råd och rekommendationer till PUA

DSO ger här samma råd som under 3.2.5 och 4.4. PUA bör se över viktiga arbetssätt och rutiner och vid behov uppdatera dem.

Men DSO råder även PUA se över vilka medarbetare som har behov av dokument och ärendehanteringssystemet eDok och att se till att medarbetare får den utbildning de behöver i systemet.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Registerförteckning (Artikel 30)
- Styrdokument

6.2 Syfte

Som nämnts ovan är det granskande arbetet en av dataskyddsombudets viktigaste uppgifter. Granskningsområdena väljs med focus 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

Registerförteckning (Artikel 30)

En registerförteckning är ett krav enligt dataskyddsförordningen. Registerförteckningen ska vara uppdaterad och aktuell.

Registerförteckningen är dataskyddsarbetets centrala utgångspunkt och bas för ett effektivt, systematiskt och riskbaserat arbetssätt. Den säkerställer att bolaget har kontroll och värnar individens integritet, särskilt när känsliga och särskilt skyddsvärda personuppgifter behandlas.

Granskningens syfte är att säkerställ att verksamheten tagit ställning till behov av konsekvensbedömning och att beslut dokumenterats.

Styrdokument

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.

Granskningens syfte är att säkerställa att lämpliga styrande dokument finns på plats och att de är uppdaterade och kända för medarbetarna.

7 Övrigt att rapportera

7.1 Granskning Fast 2

Bakgrund
I samband med en incident 2020 hos Svenska Bostäder uppmärksammades säkerhetsrisker i systemet Fast2. Dataskyddsombuden hos Svenska Bostäder, Stockholmshem, Familjebostäder och Micasa Fastigheter inledde då ett samarbete för att granska hur Fast2 uppfyllde biträdesavtalen. För genomförandet av granskningen upphandlades externa konsulter.

Granskningens resultat
Resultatet av granskningen visade att det hos Fast2 finns en okunskap om regelverket för skydd av personuppgifter.

Grundläggande processer så som riskanalys, laglig grund, behandlingsregister och gallringsrutiner saknas. Fast2 kunde inte redogöra för att ha vidtagit tillräckliga säkerhetsåtgärder.

Den registerförteckning som Fast2 lämnat uppfyller inte kraven i varken biträdesalen eller GDPR. *Artikel 30(2)*.

Enligt huvudavtalet mellan bolagen och Fast2 ska Fast2 efterfölja och uppfylla kraven i standarden ISO 270001. Fast2 uppfyller inte kraven.

Konsekvenser
Enligt Artikel 5(2) ska PUA kunna visa att dataskyddsförordningen följs, även av biträden. PUA är skyldig att endast anlita biträden som uppfyller krav och som kan lämna tillräckliga garantier om säkerhet för registrerades rättigheter. *Artikel 28(1)*.

Eftersom Fast2 inte efterföljer kraven i ISO 27001, kan de inte redogöra för ett systematiskt informationssäkerhetsarbete.

Bristerna innebär att PUA befinner sig i en situation som innebär en hög risk för incidenter relaterade till såväl personuppgiftsincidenter som övrig information.

7.1.1 DSO 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

7.1.2 DSO har gett råd och rekommendationer till PUA

Åtgärder pågår!

Bolagen har följt dataskyddsombudens råd och genom den bolagsgemensamma styrgruppen (SSG), ställt krav på Fast2. En uppföljande granskning kommer att genomföras för att säkerställa att Fast2 uppfyller kraven.

Råd som gavs

- att Fast2s ledning upprättar en registerförteckning som uppfyller krav i Artikel 30(2) GDPR.
- att Fast2s ledning upprättar en handlingsplan för övriga prioriterade dataskyddsbrister.
- att Fast2 inför ett ledningssystem för informationssäkerhet så att man uppfyller kraven i ISO 27001.

7.2 Dataskyddsgruppen

Dataskyddsförordningens krav är högt ställda och kan kännas omöjliga att uppfylla. Men målet behöver inte vara hundraprocentig efterlevnad. Det främsta målet bör vara att bolagets dataskyddsarbete är integrerat i vardagen, upprätthålls och förbättras steg för steg.

En framgångsfaktor är att arbeta systematiskt och med acceptans för frågorna i bolagets ledning.

Jag vill avsluta genom att berätta om bolagets dataskyddsgrupp som arbetar just så. Förutom DSO består gruppen av medarbetare och chefer som arbetar med informationssäkerhet, hyresgäster, personal (HR), registratur och verksamhetsutveckling. En representant från ledningsgruppen ingår.

Dataskyddsgruppen var till en början (2017) en projektgrupp inför GDPRs införande i maj 2018. Gruppens första uppgift var att inventera personuppgiftsbehandlingar, upprätta en registerförteckning och dokumentera de viktigaste rutinerna för att uppfylla de mest grundläggande kraven i GDPR.

Men för att uppfylla dataskyddsförordningens krav långsiktigt behöver arbetet fortsätta och vara systematiskt, frågorna hållas levande. Gruppen blev därför en permanent arbetsgrupp. Några nya medlemmar har tillkommit, arbetssättet har förändrats och utvecklats under åren.

Som DSO vill jag bidra genom att avdramatisera men också skapa förståelse för den grundläggande principen om varje människas rätt till skydd för sina uppgifter.

Husby 2022-01-03

Anne Tawastman

Elektroniskt undertecknad av Anne Tawastman
Datum: 2023.01.03 11:48:17 +01'00'

Anne Tawastman
Dataskyddsombud