Stockholms stad

Bilaga 6

Årsrapport över Micasa Fastigheters dataskyddshantering 2024

Januari 2025

Micasa Fastigheter

GDPR årsrapport
Januari 2025

Dnr: MIC 2024/519
Utgivningsdatum: 2025-01-02
Kontaktperson: Anne Tawastman

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 rapporten redovisas den granskning som genomförts samt hur väl organisationen uppfyller dataskyddsförordningens krav. Inga allvarliga brister har rapporterats. De brister som finns behöver åtgärdas men är inte brådskande eller omfattande.

Många nya medarbetare och förändringar i organisation, processer och rutiner kan innebära en risk för att dataskyddsarbetet får stå tillbaka. En ökad medvetenhet kring styrdokument och rutiner behöver vidareutvecklas och etableras. Här föreslås utbildnings- och informationsinsatser samt att processägare utses för samtliga processer.

Vidare redovisas rekommendationer och råd till organisationen. Att bolaget känner till var verksamheten har brister, är en viktig del i ett riskbaserat arbetssätt. Det är därför positivt att bolaget fortsätter arbetet med att nyttja de tjänster som finns i verktyget Draftit. Systemet har inbyggda funktioner som underlättar ett riskbaserat och systematiskt dataskyddsarbete. Systemet används inte bara för registerförteckning utan även för risk- och konsekvensbedömning samt incidentrapportering. Ett arbete för 2025 är att gå igenom och uppdatera registerförteckningen.

Utbildnings- och informationsinsatser behöver genomföras kontinuerligt. Under året har en nanoutbildning inom informationssäkerhetsområdet s.k. (nano-learning) genomförts. Denna kommer att genomföras även under 2025 och då också med frågor och tester kring personuppgiftshantering (GDPR).

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 slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	29 st
Har nödvändiga uppdateringar gjorts?	Ja
Bedöms registerförteckningen vara fullständig?	Ja, men kontinuerlig uppföljning och revidering behöver genomföras
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 behandla

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.

Förutom registerförteckningen som använts sedan 2020 använder bolaget även Draftit för dokumentation av incidenter och för risk- och konsekvensanalys.

DSO kontrollerar hur många behandlingar som registrerats

Bolaget har totalt 29 registreringar i registerförteckningen i Draftit.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Efter genomgång av samtliga registreringar behöver uppdateringar genomföras under 2025.

DSO bedömer hur fullständig registerförteckningen är

I registerförteckningen finns alla kända behandlingar identifierade och bedöms därför utgöra en god redovisning över bolagets personuppgiftsbehandlingar. Alla behandlingar har stöd i lag.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Ja, lämpliga rutiner finns. Dock behöver dessa kommuniceras inom bolaget. Bolagets har en dataskyddsgrupp som består av informationssäkerhetsansvarig, DSO, arkivredogörare, HR samt enhetschefer för stab, IT och kundtjänst. Dataskyddsgruppen arbetar aktivt med informationssäkerhetsfrågor och dataskydd. I gruppens ansvarsområde ingår att stödja processägarna i att uppdatera rutiner och 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 hanterar känsliga personuppgifter, till exempel hyresgästärenden och personalärenden prioriteras i

dataskyddsarbetet. Det är säkerställt att det ansvaret uppfylls. De brister som kvarstår handlar om kvalitetsförbättringar och uppdateringar.

3.1.5 DSO ger råd och rekommendationer till PUA

Micasa använder systemet Draftit för sin registerförteckning. Systemet har inbyggda funktioner som säkerställer en hög kvalitet och ger möjlighet till att identifiera risker.

Processägarnas ansvar för att uppdatering av registerförteckningen genomförs behöver tydliggöras. Då en genomgång av alla registreringar behöver genomföras under 2025 ses här möjlighet till stöd och utbildning och ökad förståelse för de behandlingar som respektive processägare ansvarar för.

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

3.2.2 Syfte

I Dataskyddsförordningen framgår att den personuppgiftsansvarige ansvarar för att arbetssätt och rutiner kring dataskyddsarbetet ska vara dokumenterade. Detta följer av att den personuppgiftsansvarige ska kunna visa att dataskyddsförordningens principer för behandling av personuppgifter efterlevs. Genom styrdokument visar personuppgiftsansvarig att det drivs ett systematiskt dataskyddsarbete.

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?

Det finns skriftliga rutiner och anvisningar för medarbetarnas dagliga arbete, hur informationen 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 göras.

Det finns anvisning för hur verksamheten arbetar med informationssäkerhet där dataskydd är en del av informationssäkerhetsarbetet.

Det finns riktlinjer för publicering av bilder och film på till exempel bolagets webbsida eller i sociala medier.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

Dokumenten som finns är ändamålsenliga, lättlästa och tydliga. För medarbetare som har kundkontakter är anvisningarna nedbrutna till konkreta ”lathundar” med exempel på vanligt förekommande problem och hur de hanteras.

Bolaget har en personuppgiftspolicy som tydligt beskriver hur skyddet av den personliga integriteten värnas.

Micasa har under 2024 bytt intranät och informationen har blivit mer lättillgänglig vilket var en brist i det tidigare intranätet.

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

Styrdokumenten finns hos bolaget men är inte kända av alla grupper. De behöver lyftas och göras mer kända. Fokus behöver läggas på chefer och ansvariga för processer för att säkerställa att dataskyddsarbetet integreras i bolagets processarbete. Positivt är att

styrdokumenten har blivit mer lättillgängliga efter byte av intranät under 2024. En del av styrdokumenten behöver 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 (vilket motsvarar de system där personuppgifter behandlas)
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.

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. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA vilket i sig utgör ett sådant stöd.

3.3.3 Resultat

Informationsklassning har genomförts för samtliga system där personuppgifter behandlas. Klassningar och uppdateringar/granskningar av samtliga historiska klassningar är påbörjade men inte slutförda under året. DSO och

informationssäkerhetssamordnaren har deltagit vid samtliga klassningar av systemen.

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

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

3.3.5 DSO ger råd och rekommendationer till PUA

Styrdokument och rutiner som rör dataskyddsarbetet bör lyftas och göras mer kända. Särskilt fokus behöver 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?	Ja
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Det har inte identifierats någon högriskbehandling inom bolaget
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.

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

3.4.3 Resultat

Bolaget har en riskmatris i systemet Draftit benämnt DPIA som används för att genomföra konsekvensbedömningar. Risk- och konsekvensbedömningen sparas i Draftit tillsammans med registerförteckningen.

Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?

Ja, Micasa har genomfört konsekvensbedömningar av de av bolaget identifierade behandlingarna. Under 2024 har två nya konsekvensbedömningar genomförts.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Micasa har inte identifierat någon högriskbehandling inom bolaget.

Är de genomförda konsekvensbedömningarna aktuella?

Ja, de genomförda konsekvensbedömningarna 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

Konsekvensbedömning är en pågående och kontinuerlig process som behöver göras regelbundet för att identifieras risker. Risken ska i första hand bedömas utifrån dataskydd och integritet. Det är viktigt att ha en hög medvetandenivå inom bolaget varför utbildning, kommunicering och information även här är en rekommendation.

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

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

Ja, förutsättningar finns att hantera registrerades rättigheter inom föreskriven tidsfrist. Hanteringen är dock manuell och kräver att handläggaren gör ett sökförfarande i alla system och register där personuppgifter hanteras. Det innebär alltid en risk för fel vid manuell hantering vilket kan betraktas som en risk.

Bolaget har förhållandevis få registrerade.

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

Det finns goda förutsättningar att hantera den här typen av förfrågningar. Då det i dagsläget är DSO som huvudsakligen hanterar förfrågningar så behöver bolaget göra en tydligare roll och ansvarsfördelning där personberoendet kan minskas. Även den manuella hanteringen av sammanställningen behöver ses över. På så sätt minskar risken som den manuella hanteringen utgör.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Genom stickprovskontroller och anmälan från medarbetare inom bolaget.
Hur många personuppgiftsincidenter har dokumenterats?	5
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Inga
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	-

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 dataskyddsförordningen. Incidenthanteringen består av två huvudsakliga moment – rapportering respektive dokumentation. Även i de fall som incidenten inte ska rapporteras till IMY så behöver alla personuppgiftsincidenter dokumenteras. Omständigheterna, dess effekter och korrigerande åtgärder ska ingå i dokumentationen.

Bristande dokumentering är sanktionsgrundandande.

3.6.3 Resultat

Hur väl förmår verksamheten att rapportera personuppgiftsincidenter i tid till Integritetsskyddsmyndigheten?

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. Det finns ett högt incidentmedvetande bland bolagets medarbetare.

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

Inga.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- *Rutin och hantering av personuppgiftsbiträdesavtal vid upphandling*
- *Finns utsedda informationsägare*

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 fokus 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

- *Rutin och hantering av personuppgiftsbiträdesavtal vid upphandling*

För att säkerställa att inga upphandlingar medför att Micasa Fastigheter upplåter åt personuppgiftsbiträden att behandla personuppgifter utan att korrekta personuppgiftsbiträdesavtal upprättats så behöver det finnas en rutin/arbetssätt som tillämpas. Inköpsenheten har ingen rutin men det finns en mall och checklista som används vid startmöten inför upphandlingar för att säkerställa att personuppgiftsbiträdesavtal upprättas vid behov. Under 2025 kommer arbetssätten att ses över och utbildningsinsatser att genomföras.

	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

- *Finns utsedda informationsägare*

För att säkerställa att processer där personuppgifter hanteras, klassas och risk- och konsekvensbedöms ska informationsägare finnas utsedda. Granskningen syftar till att undersöka ifall informationsägare finns utsedda för samtliga processer. Informationsägare finns för de processer som hanterar personuppgifter. Informationsägare för övriga verksamhetsprocesser behöver utses.

	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

Inköpsenheten behöver se över arbetssätt och genomföra utbildningsinsatser för att säkerställa att personuppgiftsbiträden inte behandlar personuppgifter utan att korrekta personuppgifts-biträdesavtal upprättats.

Bolaget behöver gå igenom alla kända processer och tillse att informationsägare finns utsedda för samtliga även de som inte innehåller personuppgifter.

5 Risker inom dataskydd

5.1 Sammanfattning

Det finns inga allvarliga brister i dataskyddshanteringen men det finns förbättringspotential när det kommer till att tydliggöra verksamhetens ansvar och skyldigheter.

5.2 Syfte

Micasa Fastigheters dataskyddsgrupp arbetar med att stödja verksamheten med dataskyddsarbetet inom bolaget. Då främst denna grupp arbetar med dataskyddsfrågor så finns en risk att ansvar och större delaktighet inte finns i verksamheten i det löpande dataskyddsarbetet.

5.3 Resultatet av riskkartläggningen

Incidenter som uppmärksammats under 2024 har handlat om att personuppgifter sparats på ett felaktigt sätt eller mejlats vidare inom bolaget. För registrerade personer har bristerna inte inneburit några personliga konsekvenser.

	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

Risk 2

Omedvetenhet kring rutiner och styrdokument kring dataskyddsarbetet. Här behöver löpande information och utbildningsinsatser genomföras.

	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

5.4 DSO ger råd och rekommendationer till PUA

Gallring och arkivering av information framför allt på gruppdiskar behöver genomföras minst en gång per år. I verksamhetsplanen för 2025 har arbetet med arkivering och gallring lagts som fokusområde för hela bolaget. Det är en del i ett större informationsprojekt som bl.a. rör fastighetsinformation och som innebär att bolaget behöver gå över till att arbeta mer med information i system än på gruppdisk. Positivt är att alla medarbetar nu har behörighet i eDok och kan hantera känslig information med markering för både sekretess och känsliga personuppgifter. Utbildningsinsatser i eDok behöver dock genomföras kontinuerligt. I januari uppgraderas eDok till en ny version och då kommer det hållas öppet hus löpande under året för introduktioner och erbjudas utbildningar.

Särskilda utbildningsinsatser och information till chefer och processägare behöver genomföras 2025. Även om processägare är utsedda för de processer där personuppgifter hanteras så behöver bolaget utse processägare för samtliga processer. Vidare behöver bolaget fortsätta med nano-utbildningar för alla medarbetare. Positivt är att det även under år 2025 kommer att erbjudas nano-utbildningar där utbildningen kompletteras med frågor/tester för personuppgiftshantering.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Information till registrerade*

6.2 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.

Granskning 2025

Under 2025 ska en granskning ske över hur information till registrerade ges och vad informationen innehåller. Särskilt ska vi granska hur informationen ser ut till seniorhyresgäster, verksamheter och anställda som kvitterar ut elektroniska nycklar (aptus). Det har att göra med integriteten gällande de loggar som registreras vid passage.

7 Övrigt att rapportera

7.1 Sammanfattning

Under hösten 2023 genomfördes organisationsförändringar som fick genomslag under 2024. Nya arbetsformer och roller infördes samt att personalen fortsatt kan arbeta på distans om arbetet tillåter. Detta i kombination med att en hel del nya medarbetare har anställts kan medföra risker att dataskyddsinformationen inte når ut till alla anställda eller att dataskyddsarbetet inte prioriteras. Vidare att bolaget har vuxit i kombination med distansarbete så har det traditionella sättet att utbilda på plats utmanats.

Bolaget har för att möta utmaningarna genomfört insatser genom digitala utbildningar (stadens obligatoriska digitala utbildningar inom dataskydd- och informationssäkerhet) samt kortare och riktade utbildningar/tester som så kallade nano-utbildningar (nano-learning). Detta kommer att fortsätta under 2025 och då också med riktade frågor kring personuppgiftshantering och dataskydd. Vidare har månadsvisa introduktioner för nyanställda genomförts.

Säkerställande av kunskapsnivå för dataskyddsarbetet är nödvändigt. Dataskyddsgruppen spelar här en central roll för stöd och utbildning samt att chefer följer upp att nya medarbetare genomför de obligatoriska digitala utbildningarna inom dataskydd och informationssäkerhet.

7.2 DSO ger råd och rekommendationer till PUA

Inga ytterligare råd och rekommendationer.