Stockholms stad

Årsrapport över Micasa Fastigheters dataskyddshantering

Januari 2024

Micasa Fastigheter

Micasa Fastigheters årsrapport
Januari 2024

Dnr: MIC 2023/614
Utgivningsdatum: 2024-01-09
Kontaktperson: Marie Eriksson

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 ledningsnivå.

Denna årsrapport är således ett medel för styrelsen att ta emot råd och rekommendationer enligt dataskyddsförordningen samt för att få insyn i det granskande arbetet av verksamhetens status avseende integritet och dataskydd visar. Detta för att nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Samspelet resulterar i att det blir enklare för ansvarig bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

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

Innehåll

Innehåll

2 Sammanfattning

I rapporten redovisas den granskning som genomförts samt hur väl organisationen uppfyller dataskyddsförordningens krav. Vidare redovisas rekommendationer och råd till organisationen där brister påvisats.

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.

Alla medarbetare måste genomföra en obligatorisk utbildning i dataskydd och informationssäkerhet. Därigenom finns en medvetenhet inom bolaget om dataskyddsförordningens krav. Under året har en särskild satsning genomförts inom informationssäkerhetsområdet s.k. (nano-learning).

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 efter genomförd granskning samt rekommendationer.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	28 registreringar *(22 året innan)*
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 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 under 2023. Det har skett i samband med att nya system eller systemstöd 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 några av behandlingarna.

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

3.1.4 Nedan anges 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, t ex 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 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, är ett fortlöpande och återkommande arbete.

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 utbildning och att skapa kännedom om dem behöver genomföras kontinuerligt
Är dokumenten uppdaterade?	Ja, huvuddelen av dokumenten är uppdaterade
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja, processägare är utsedda som också har ansvar för uppdateringar

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/beskrivning vad som menas med inbyggt dataskydd och dataskydd som standard i verksamhetens processer och rutiner.

Det finns riktlinjer för publicering av bilder och film på t ex 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. Under 2023 har arbetssätt och rutiner uppdaterats på intranätet för få en bättre översikt av alla styr-/stöddokument.

3.2.4 Nedan anges 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 Råd och rekommendationer till PUA

Behov av uppdatering
Förra årets DSO-rapport pekade på förbättringsområden kring struktur och överskådlighet för rutiner, dokument och anvisningar. DSO menade att informationen var svåröverskådlig.

Under 2023 har ett förbättringsarbete genomförts.
Sidorna på intranätet har blivit mer överskådliga och lättillgängliga. Struktur för hur rutiner, dokument och anvisningar presenteras har uppdaterats.

Det är positivt att arbetssätt och rutiner tydliggjorts samt att informationssidor på intranätet har samordnats och skapat en bättre översikt.

En beskrivning behöver tas fram vad som menas med inbyggt dataskydd och dataskydd som standard.

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?	4 nya klassningar har genomförts. Ingen revidering av övriga klassningar har genomförts.
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 2023 har bolaget tagit fram en lokal anvisning för informationssäkerhet. Den beskriver roller och organisation för informationssäkerhetsarbetet samt hur Micasa systematiskt arbetar med och följer upp informationssäkerheten.

3.3.4 Nedan anges 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?	Någon högriskbehandling har inte identifierats hos 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.

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

Micasas modul i Draftit togs i bruk 2022 och den används fortsatt för att genomföra konsekvensbedömningar. Bedömning och dokumentation sparas nu samlat tillsammans med registerförteckningen i Draftit.

3.4.4 Nedan anges 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 Råd och rekommendationer till PUA

Arbetat med att identifiera risker behöver fortsätta och riskbedömningen behöver gås igenom årligen och revideras för samtliga processer. Särskilt fokus behövs gällande de processer där känsliga personuppgifter hanteras (t ex störningar i boendet). All bedömning ska dokumenteras i 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 Nedan anges 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?	Genom DSOs stickprovskontroller och anmälan från medarbetare och chefer till DSO.
Hur många personuppgiftsincidenter har dokumenterats?	4
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 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:

- Registerförteckning (Artikel 30)
- Styrdokument

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

Registerförteckning

En registerförteckning är ett krav enligt dataskydds-förordningen. 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 dataskyddsarbetet.

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.

4.4 DSO ger råd och rekommendationer till PUA

Registerförteckning, (Artikel 30)

Micasa Fastigheter har en registerförteckning i systemet Draftit.

I Micasas registerförteckning redovisas alla bolagets processer och system där personuppgifter hanteras. Bolaget använder Draftits modul som stödverktyg för registerförteckningen. Konsekvensbedömningar finns registrerade och dokumenterade i Draftit.

Micasa har således visat att bolaget har kontroll och överblick över alla kända personuppgiftsbehandlingar. Det finns dock några behandlingar i registerförteckningen som ligger i granskningsläge och dessa behöver slutföras och slutmarkeras.

Dataskyddsgruppen har under 2023 gått igenom styrdokumenten för Micasas personuppgiftsbehandlingar. Det finns en personuppgiftspolicy samt rutiner för hantering av personuppgifter och personuppgiftsincidenter samt instruerande lathundar samt gallringsregler. Sidorna där informationen presenteras har uppdaterats under året och informationen har blivit mer överskådlig. Under året har även en lokal anvisning för informationssäkerhetsarbetet tagits fram, se tidigare avsnitt.

Micasa medvetandegör policys och rutiner för medarbetarna genom introduktion av nya medarbetare, samt att alla medarbetare ska genomgå en obligatorisk digital utbildning i dataskydd och informationssäkerhet. Vid ett av bolagets informationsmöten under året deltar DSO och undervisar och informerar om bolagets hantering 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
	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, tredje-landsöverföringar, 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 uppmärksammats under 2023 har handlat om att personuppgifter sparats på ett felaktigt sätt. För registrerade personer har bristerna inte inneburit några personliga konsekvenser.

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

Dataskyddsgruppens rekommendationer är att löpande arkivera och gallra information från gruppdiskar och samarbetsytor. Dataskyddsgruppen råder PUA att rekommendera att dokument- och ärendehanteringssystemet eDok används och säkerställa att medarbetare får utbildning i systemet.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Rutiner och hantering av personuppgiftsbiträdesavtal vid upphandlingar
- Uppföljning att det finns utpekade personer som är informationsägare inom bolaget

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

Rutiner och hantering av personuppgiftsbiträdesavtal vid upphandlingar

För att säkerställa att inga upphandlingar medför att Micasa Fastigheter upplåter åt personuppgiftsbiträden att behandla personuppgifter utan att korrekta personuppgiftsbiträdesavtal upprättats kommer en granskning att genomföras för att säkerställa att rutin finns samt att särskilda utbildningsinsatser har genomförts. Granskningens syfte är således att säkerställa att verksamheten tagit ställning till behov av konsekvensbedömning och att beslut dokumenteras.

Uppföljning att det finns utsedda personer/roller som är informationsägare inom bolaget

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.