Stockholms stad

GDPR Årsrapport

År 2023

AB Stockholmshem

GDPR årsrapport
Januari 2024

Utgivningsdatum: 2023-12-20
Kontaktperson: Fredrik Beckman

1 Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

Enligt dataskyddsförordningen är varje nämnd och bolagsstyrelse inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnd och bolagsstyrelse behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett Dataskyddsombud (”DSO”). DSO:n har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är således ett medel för nämnd och styrelse att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

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

Innehåll

2 Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

Till att börja med vill jag säga att inga allvarliga brister rapporteras. De brister som finns bör åtgärdas, men bedöms inte vara brådskande eller omfattande.

Många nya medarbetare och förändringar i organisation och rutiner kan innebära en risk för att det systematiska dataskyddsarbetet får stå tillbaka. Särskilda utbildningsinsatser har därför genomförts på enheter/avdelningar som har särskilt hög omsättning, som t.ex. kundtjänst.

Ett arbete med att säkerställa att information på och om Dataskydd snabbt ska kunna nå ut även till nyanställda har genomförts och systematik för att information/utbildning skall nå ut till samtlig personal även digitalt har lagts ner och börjat användas under 2023.

Registerförteckningen för behandlingar av personuppgifter är central och viktig. En överflyttning in i systemstödet, DraftIt, som har inbyggda funktioner som underlättar ett riskbaserat och systematiskt dataskyddsarbete skulle underlätta för bolagets fortsatta dataskyddsarbete.

För dataskyddsarbetet är ansvar och roller beskrivna och det finns dokumenterade anvisningar och rutiner. Det finns däremot ett stort behov att löpande kommunicera rutinerna och anvisningarna. Dataskyddsarbetet bör lyftas för att bli en självklar rutin i hela organisationen.

DSOs uppdrag är bland annat att granska hur väl organisationen uppfyller dataskyddsförordningens krav, samt att informera och ge råd till organisationen. För mig som DSO är det glädjande att verksamheten i hög stor utsträckning vänder sig till mig med hanteringsfrågor och att man även tar till sig och följer de råd jag ger. Min upplevelse är att verksamheten har en hög ambition och vilja att göra rätt i dessa frågor.

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 nämndens eller bolagets status och DSO:ns slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:ns genomförda uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	80
Har nödvändiga uppdateringar gjorts?	JA
Bedöms registerförteckningen vara fullständig?	JA
Har verksamheten lämpliga rutiner för registerföring?	NEJ

3.1.2 Syfte

Av Dataskyddsförordningen (artikel 30) så skall bolaget ha inventerat alla personuppgifter som behandlas i verksamheten både i rollen som personuppgiftsansvarig och personuppgiftsbiträde och dokumentera detta i en så kallad registerförteckning.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

En särskild genomgång av så väl omfattningen som de enskilda delarna av registerförteckningen har genomförts under hösten 2023.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Med anledning av den genomgång som genomförts under hösten har även nödvändiga uppdateringar genomförts i registerförteckningen.

DSO bedömer hur fullständig registerförteckningen är

Registerförteckningen bedöms utgöra en god redovisning över de behandlingar som finns i bolaget.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Ett systematiskt och verksamhetsförankrat arbetssätt för registerförteckningen saknas. En registerförteckning får inte vara ett statiskt dokument och återspegla de behandlingar som görs hos bolaget i varje enskilt ögonblick och DSO bedömer därför att även om registerförteckningen isig är fullgod så finns det förbättringsmöjligheter med ett framtida bättre systematiskt arbetssätt.

3.1.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	Inga brister av nämnvärd betydelse identifierade

3.1.5 DSO ger råd och rekommendationer till PUA

Det fortsatta Dataskyddsarbetet på bolaget bör lägga in uppdateringar av registerförteckningen som en naturlig del i verksamhetens löpande arbete.

Registrering av processer där personuppgifter behandlas är att föredra framför registrering av enskilda behandlingar. Det ger en bättre överblick och förenklar det dagliga arbetet. Bolaget behöver inte särskilja varje moment där personuppgifter behandlas, utan kan göra en samlad registrering för en viss process. Ansvar för att registerförteckningen verkligen hålls uppdaterad bör ligga hos ansvarig för respektive process.

Detta genomförs lämpligast som den del av arbetet med att överföra registerförteckningen till det tillgängliga systemstödet DraftIT, som isig ger stöd i ansvarsfrågor för respektive behandling samt förbättrad synlighet av de enskilda delarna av registerförteckningen.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Ja, till stor del
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Ja
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Ja
Är dokumenten uppdaterade?	Ja
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja

3.2.2 Syfte

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.

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.

DSO bedömer om innehållet i existerande dokument håller 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 Stockholmshem värnar om skyddet av den personliga integriteten.

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.

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

Genom styrdokument visar PUA att det bedrivs ett systematiskt dataskyddsarbete, men styrdokumenten måste även vara kommunicerade. Styrdokument finns hos bolaget, men de är inte kända i alla grupper.

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

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?	47 (vilket motsvarar de system där personuppgifter behandlas)
Är klassade personuppgiftsbehandlingar aktuella?	JA, men rutin för årlig uppföljning av eventuella handlingsplaner saknas

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 isig möjliggör ett sådant stöd.

3.3.3 Resultat

Informationsklassning har genomförts för samtliga system där personuppgifter behandlas. Klassningar och uppdateringar/granskningar av samtliga historiska klassningar påbörjad men ej slutförd under året. DSO har deltagit i 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.

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

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 dataskydd bör lyftas och göras mer kända. Särskilt focus 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?	Ja
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Ja
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 ska sedan riskförebyggande åtgärder vidtas.

3.4.3 Resultat

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

Ja

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Ja

Är de genomförda konsekvensbedömningarna aktuella?

Ja

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

En konsekvensbedömning ska alltså göras om en viss personuppgiftsbehandling "sannolikt leder till en hög risk för fysiska personers rättigheter och friheter". Risken ska i första hand bedömas utifrån dataskydd och integritet, men även utifrån andra grundläggande rättigheter som yttrandefrihet, tankefrihet, fri rörlighet, förbud mot diskriminering, rätt till frihet, samvete och religion.

Konsekvensbedömningen är en pågående process, inte en engångsaktivitet som skall genomföras vid ett enda tillfälle. En hög medvetandenivå inom bolaget om detta är naturligtvis viktig och även om detta idag inte brister så är det viktigt att kontinuerligt arbeta vidare med denna fråga.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	4
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	4

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 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

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

Rutin och hantering av begäran om registerutdrag finns kommunicerade på bolagets intranät. Det krävs ett manuellt handhavande vid framtagandet av registerutdraget och DSO har därför själv personligen hanterat samtliga sådana förfrågningar.

Samtliga förfrågningar har hanterats inom förordningens angivna tidsfrist.

Utöver de regelrätta registerutdragsförfrågningarna så har naturligtvis även ett större antal övriga förfrågningar hanterats från registrerade, men dessa har egentligen handlat om begäranden om offentliga handlingar och inte varit direkt kopplade till den registrerades personuppgifter.

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

Även om goda förutsättningar att hantera denna typ av förfrågningar finns på bolaget och så bör bolaget ändå göra en förbättring i form av att personberoende bör ersättas av en tydligare roll och ansvarsfördelning. Där även de manuella moment som idag görs för sammanställningen bör ses över. Detta för att i framtiden höja säkerheten ytterligare.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Teoretiskt av bolagets personal, genom DSOs kontroller eller efter information från staden, samt i värsta fall efter det att någon drabbad hör av sig.
Hur många personuppgiftsincidenter har dokumenterats?	3
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	1
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	1

3.6.2 Syfte

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

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

Bolaget har uppsatta rutiner för att hantera situationer då incident misstänks eller rapporteras till utpekad grupp.
Information om hanteringen finns tillgänglig på bolagets intranät och medarbetare utbildas i att känna igen personuppgiftsincidenter

och hur de anmäls. Att medarbetare hör av sig med anledning av denna rutin oavsett om det rör sig om det i sig inte handlar om en incident tolkar jag som att incident medvetande finns bland bolagets personal.

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:

- Särskild genomgång av bolagets registerförteckning
- Granskning av åtgärder som följd av tidigare genomförd säkerhetsgranskning inkl. penetrationstest av interna verksamhetssystem från extern åtkomst
- Rutiner och hantering av personuppgiftsbiträdesavtal vid upphandlingar

4.2 Syfte

Under året har framför allt insatser genomförts för att säkerställa att nödvändiga åtgärder vidtagits med anledning av historiskt upptäckta risker.

4.3 Genomförda granskningar och deras resultat

- Särskild genomgång av bolagets registerförteckning

Bolagets registerförteckning uppfyller i sig lagstiftningens uppställda krav.

	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

- Åtgärder som följd av tidigare genomförd säkerhetsgranskning inkl. penetrationstest av interna verksamhetssystem från extern åtkomst

Säkerhetsgranskningen syftade till att verifiera att definierade säkerhetsklassningar och skyddsnivåer är verkligen är uppfyllda och

att systemen uppfyller de definierade säkerhetskraven. De vid tidigare genomförda säkerhetsgranskningar påtalade teoretiska brister som funnits har alla täppts till.

	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

- Rutiner och hantering av personuppgiftsbiträdesavtal vid upphandlingar

För att säkerställa att inga upphandlingar medför att Stockholmshem upplåter åt personuppgiftsbiträden att behandla personuppgifter utan att korrekta personuppgiftsbiträdesavtal upprättats för behandling så har dels rutinen tydliggjorts och särskilda utbildningsinsatser har genomförts med Inköp.

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	Inga brister av nämnvärd betydelse identifierade

4.4 DSO ger råd och rekommendationer till PUA

Inga särskilda föranledda av granskningen.

5 Risker inom dataskydd

5.1 Sammanfattning

Dataskyddsombudets egen kartläggning har inte påvisat några alvarliga brister, men kan se tydlig förbättringspotential när det behov av att tydliggöra verksamhetens ansvar och skyldigheter.

5.2 Syfte

Det finns en risk inbyggd i att ansvar och större delaktighet inte finns i det löpande dataskyddsarbetet på bolaget.

För att bedöma risker har dataskyddsombudet genomfört en egen riskkartläggning med stöd av stadens riktlinjer och lämnat nedanstående förbättringsförslag.

5.3 Resultatet av riskkartläggningen

	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

Det uppstartade arbetet med att skapa och kontinuerligt verka med dataskyddsfrågor i den större arbetsgruppen med utpekade ansvar för verksamhetens egna processer bör fortsätta. Utpekade representanter finns som alla har tackat ja när de tillfrågats. Särskilda utbildningsinsatser har därför redan bokats in med gruppen i början av nästa år. DSO´s rekommendation är därför att detta delvis förändrade arbetssätt skall få arbetas in under kommande år, enär det redan är påbörjat.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Granskning av verksamhetssystem

6.2 Syfte

Det granskande arbetet utgör en av Dataskyddsombudets viktigaste uppgifter. Under kommande år så avser jag att framför allt genomföra granskande arbete på behandlingen av vår största personuppgiftskategori dvs våra hyresgäster.

6.3 Planerade granskningar

Granskning av verksamhetssystem

Den beställda externa granskningen av Fastighetssystemet Fast2 som påbörjats under 2021 och slutfördes under 2022 kommer det fortsatt arbetas med. Granskning av att framkomna åtgärder gällande framför allt förändringen av stödet för sekretesshanteringen fortskrider med åtgärder som skall genomföras.

7 Övrigt att rapportera

7.1 Sammanfattning

Under 2023 genomfördes organisationsförändringar, nya arbetsformer infördes och en stor del av personalen har fortsatt att arbeta på distans, mycket som en följd av Pandemin. Detta i kombination med att många nya medarbetare anställts har inneburit att den mera traditionella katederundervisningen inte har kunnat genomföras i en sådan omfattning som skulle ha varit önskvärt. Vilket i sig innebär en risk för att dataskyddsinformation inte säkerställt når ut till all anställda.

Som komplement till den traditionella på plats utbildning så har sedan 2022 särskilda digitala insatser genomföras i form av mera

traditionella digitala utbildningar/tester men också i form av kortare riktade så kallade Nano-utbildningar. Detta tror jag utöver en större verksamhetsförankring i form av uppstart av en större organiserad dataskyddsgrupp är en framgångsfaktor för bolaget.

7.2 Syfte

Säkerställandet av kunskapsnivå och förståelsen för dataskyddsarbete är nödvändigt för ett framgångsrikt dataskyddsarbete.

7.3 Övriga observationer

Tidigare absoluta stopp för molntjänster har i och med EU-beslut möjliggjorts men eftersom rättsläget framåt är fortsatt osäkert och snabbt kan ändras så råder fortsatt försiktighet rörande införande av dessa.

7.4 DSO ger råd och rekommendationer till PUA

Inga ytterligare råd eller rekommendationer

Fredrik Beckman
Dataskyddsombud
AB Stockholmshem

Attesterat av

Detta dokument har godkänts digitalt av följande personer:

Namn	Datum
Åsa Wigfeldt, VD	2024-01-25