Rapport

DNR FB 2024/1236

2024-12-19

Dataskyddsombudets årsrapport 2024

AB Familjebostäder Box 92100 120 07 Stockholm 08-737 20 00 växel 0770-814 814 kundservice kontakt@familjebostader.com www.familjebostader.com

Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

År 2024 var året som AI-verktygen började implementeras i IT-tjänster där man minst kunnat ana det tidigare. Den nya lagen om AI, AI förordningen, antogs i EU under våren och kommer implementeras under de kommande tiden i olika faser. Ur ett dataskyddsperspektiv blir frågorna än mer intressanta och komplexa i och med att AI:n skapar nya personuppgiftsbehandlingar. Det är också uppmärksammat att ett antal incidenter har skett i staden under året då nya AI:n implementerats av misstag i olika digitala verktyg vid uppdateringar. En av de granskningar jag prioriterat är just AI och integritetsproblematiken. familjebostäder har börjat med att ta fram styrdokument och metoder för att kunna göra analyser innan ett införande av en IT-tjänst med AI-funktioner. Ett bra exempel på att organisationen vill effektivisera på rätt sätt med en hänsyn till individen.

Samhället har påverkats av flera uppmärksammade incidenter, bland annat en större ransomware-attack hos TietoEvry i januari 2024. Incidenten skapade stor oro och informationen var otydlig till en början. Turligt nog klarade sig Stockholm stad i den attacken, men andra kommuner drabbades samtidigt mycket hårt. I min rapport för år 2023 spådde jag att det fortsatt skulle bli prioriteringar inom kontinuitetsplanering för hela Stockholm stad vid kris och krig. Familjebostäder har startat ett större projekt inom detta område under 2024. Detta var ett av mina granskningsområden under det gångna året men jag ser en större nytta att flytta denna granskning ett år framåt då det kommit än längre.

Under år 2025 hoppas jag på att kunna fokusera än mer på riskhantering och öka mognaden inom organisationens dataskyddsarbete. Idag är det oftast knutet till individers enskilda kunskaper och blir i sig en risk i det systematiska arbetet. Kunskapen om dataskydd är en färskvara och under 2024 har endast 24 % av medarbetarna genomgått den *obligatoriska* digitala utbildningen. En acceptabel nivå är ca 80 %.

Ni är en bra bit på väg men man blir aldrig färdiga!

Jessica Hillergård

Dataskyddsombud

Innehållsförteckning

1 Inledning

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 styrelse 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. Denna roll 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 styrelsen att ta emot de råd och rekommendationer som dataskyddsombudet är skyldig att ge till ansvarig enligt dataskyddsförordningen. I rapporten får styrelsen insyn i vad dataskyddsombudets granskningar visat av verksamheten och status avseende integritet och dataskydd. Årsrapporten syftar till att styrelsen ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig styrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

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

2 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som personuppgiftsansvarig, PUA, som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som dataskyddsförordningen avser.

De obligatoriska rapporteringsområdena är:

- registerförteckning
- styrdokument
- tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar
- konsekvensbedömningar
- individens rättigheter
- personuppgiftsincidenter

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

2.1 REGISTERFÖRTECKNING

2.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	147
Har nödvändiga uppdateringar gjorts?	Nej
Bedöms registerförteckningen vara fullständig?	Ja
Har verksamheten lämpliga rutiner för registerföring?	Nej

2.1.2 Syfte

För att något ska gå att skydda måste det först vara synligt för verksamheten. Det följer därför i klartext av dataskyddsförordningen (artikel 30) att stadens alla förvaltningar och bolag måste inventera alla personuppgifter som behandlas i verksamheten, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde, och dokumentera dem i en så kallad registerförteckning (även kallat behandlingsregister eller register av register).

När registerförteckningen är upprättad skapar den en intern synlighet och förståelse för vilka personuppgifter som behandlas samt hur de hanteras. Registerförteckningen är därför dataskyddsarbetets centrala utgångspunkt och bas samt säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling. Det är därför viktigt att PUA får information om hur komplett verksamhetens förteckning är. Om dokumenteringskravet uppfylls kan verksamheten arbeta effektivt, systematiskt och riskbaserat och samtidigt värna om individens integritet, särskilt när känsliga och särskilt skyddsvärda personuppgifter behandlas av verksamheten.

Att ha en registerförteckning på plats leder till att verksamheten kan arbeta mer resurs- och kostnadseffektivt med sitt systematiska och riskbaserade dataskyddsarbete. Man kan styra insatserna där de gör störst nytta.

Syftet med detta rapporteringsområde är således att rapportera till PUA hur väl verksamhetens har lyckats inventera sina personuppgifter och de personuppgifter som behandlas för annans räkning och upprätta en registerförteckning.

Eftersom inventeringen av personuppgifter i sig är avgörande för allt det fortsatta dataskyddsarbetet inom verksamheten, är denna lägesbild en av de viktigaste slutsatserna som PUA behöver förstå och ta ställning till inför det planerade åtgärdsarbetet under nästa verksamhetsår.

2.1.3 Resultat

Registerförteckningen i finns i ett digitalt verktyg kallat DraftIt och består av ett frågeformulär per personuppgiftsbehandling vilket i sin tur blir funktionen av en checklista att alla krav i GDPR dokumenteras korrekt.

Registreringarna utgår från hanteringsanvisningen och dess processer och har fått utpekade ansvariga utifrån processägarskapet. Rutin finns beskriven med ansvarsfördelning på Porten. Dock sker endast uppdateringar ad hoc och på efterfrågan av DSO.

2.1.4 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

2.1.5 DSO ger råd och rekommendationer till PUA

Vid den pågående kartläggningen av processägare och i kontinuitetsprojektet, uppmanas Familjebostäder att även lyfta in kontroll och uppdatering av registerförteckning i det arbetet. Syftet är att få systematik och minska personberoendet.

2.2 STYRDOKUMENT

2.2.1 Sammanfattning

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

2.2.2 Syfte

Området syftar till att PUA genom styrdokument ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar PUA till medarbetare i sin verksamhet om vad som gäller och vad som förväntas av medarbetarna, när de hanterar personuppgifter. 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. 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 (artikel 5).

Rapporteringen av området är tvådelad: dels ska DSO bedöma om verksamheten har de styrdokument antagna och på plats, dels ska rapporteringen visa om dokumentationen innehållsmässigt håller en lämplig kvalitet, i vilket ingår bl.a. att dokumentationen ska vara uppdaterad och aktuell.

En brist inom detta område bör förstås ses som en brist i förhållande till direkta lagkrav, men det finns fler nyanser av detta som bör lyftas fram till PUA. Bristande styrning på grund av att lämplig styrande dokumentation saknas leder exempelvis ofta till bristande kvalitet i hur verksamheten utför aktiviteterna, men

även till att verksamheten slösar värdefulla resurser när exempelvis för många personer blir involverade i en incidenthantering eller för att en analys behöver göras om från grunden varje gång istället för att man återanvänder redan uppfunnen kunskap. Dessa effekter drabbar verksamheter ur ett vidare perspektiv och är något som ligger i PUA:s intresse att förstå för att fatta rätt beslut om.

2.2.3 Resultat

Familjebostäder har egen handledning för hur personuppgiftsincidenter ska hanteras samt en förklaring om vad GDPR/ Dataskyddsförordningen innebär. Dessa finns publicerade på Familjebostäders intranät, Porten. Innehållet på intranätet är gediget och länkar även vidare till tillsynsmyndighet och viktiga vägledningar. Lokal tillämpningsanvisning för informationssäkerhet har antagits under 2024 och även styrdokument kring implementering av AI.

Brister finns identifierade på externwebben där kakor-policyn inte är korrekt och hänvisar till fel personuppgiftsansvarig. Det skiljer också i startsidans information om kakor och Familjebostäders egen sida ”vår användning av kakor[1]”. Förändringen ser ut att ha skett hösten 2024 och DSO har inte tillfrågats om råd i detta ärende.

2.2.4 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

2.2.5 DSO ger råd och rekommendationer till PUA

Familjebostäder måste åtgärda kakor-policyn så snart som möjligt och förtydliga vilken policy, banner och kakor som hämtas in i informationen till den registrerade.

[1] https://www.familjebostader.com/om-familjebostader/om-webbplatsen/om-kakor/ (2024-12-17)

2.3 TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER FÖR PERSONUPPGIFTSBEHANDLINGAR

2.3.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	För 2024 3 st. fullständiga klassningar och 20 st. förklassningar
Är klassade personuppgiftsbehandlingar aktuella?	Ja

2.3.2 Syfte

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. Utan informationsklassningen har verksamheten inte förutsättningar att välja rätt åtgärder för att skydda sin information. Det är därför av stor betydelse för dataskyddsarbetet att PUA ges en uppdaterad bild varje år av huruvida informationsklassning är genomförd för personuppgifter som verksamheten hanterar.

Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare. En första kontrollpunkt måste därför vara om en informationsägare eller en informationsägarrepresentant med ansvar för klassning är identifierad i verksamheten. Om en ansvarig för klassningen inte har pekats ut och känner till sitt ansvar för klassning, minskar sannolikheten avsevärt att en klassning faktisk initieras.

Notera att enbart sådan informationsklassning som avser behandling eller system som omfattar personuppgifter är av intresse för DSO:s årsrapportering.

Viktigt är också att notera att dataskyddsombudet omhändertar den registrerades intresse och informationssäkerhetssamordnaren har fokus på verksamhetens krav på informationen i form av tillgänglighet, riktighet och konfidentialitet. Verktyget för DSO är i första hand registerförteckningen och dokumentationen där. Informationssäkerhetssamordnaren har KLASSA som verktyg för att se till att verksamhetens krav efterlevs i form av dokumentation i förvaltningsplaner, systembeskrivningar etc.

Eftersom informationsklassning är ett arbete som görs inom ramen för informationssäkerhetsarbetet, bör DSO samråda och planera uppföljningen tillsammans med informationssäkerhetssamordnare. Enligt stadens metodik klassas personuppgifter och övrig information i samma workshop, och slutsatserna kring klassningen dokumenteras i samma protokoll.

2.3.3 Resultat

Metodiken att informationsklassa med förklassningsprotokoll och därefter i det digitala verktyget KLASSA har fortsatt vara metod inom Familjebostäder. Verktyget KLASSA har också utvecklats utifrån dataskyddet under 2024 av SKR och är nu mer definierat än tidigare. Detta ger en möjlighet för verksamheten att arbeta med mer av en checklista än tidigare versioner av analysresultat av KLASSA.

Samtliga personuppgiftsbehandlingar klassas utifrån vilken typ av personuppgifter som behandlas och lämpligt skydd vidtas för respektive behandling. Detta kan vara behörighetsbegränsning, skydd av lösenord på dokument osv. Detta dokumenteras i DraftIT. En klassificeringsstruktur med märkning av dokument finns inte.

2.3.4 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

2.3.5 DSO ger råd och rekommendationer till PUA

Informationsklassning sker fortfarande med ett beroende av att nyckelpersoner finns att tillgå och enskilda individers intresse. Mognaden är låg och med införandet av kontinuitetsarbete och förvaltarmodellen för informationssäkerhet behöver detta bli mer tydligt i ansvarsfördelningen vem som gör vad och att det finns tid avsatt för ansvarsområdena.

Rekommendationen från DSO är att fortsätta se till nästa steg i införandet av förvaltningsmodellen för informationssäkerhet är att klassificera de processer som ingår i hanteringsanvisningen. Identifierar man processer och inte ser endast till system, blir klassningen av information/ personuppgifterna än mer konkret och verklig.

2.4 KONSEKVENSBEDÖMNINGAR

2.4.1 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

2.4.2 Syfte

Konsekvensbedömningen hjälper en organisation att identifiera och minimera integritetsriskerna för personuppgifter som behandlas i projekt eller linjeverksamhet. 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. Baserat på bedömningen kan/ ska riskförebyggande åtgärder vidtas.

Konsekvensbedömningen anses liksom registerförteckning och informationsklassning som ett viktigt verktyg för verksamhetens dataskyddsarbete. Kravet på konsekvensbedömning är dessutom ett uttryckligt krav enligt dataskyddsförordningen och ska utföras för alla behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1).

2.4.3 Resultat

Organisationen arbetar med konsekvensbedömningar. Rutiner finns på plats på intranätet, Porten. Aktiviteten sker dock individberoende, d.v.s. individer har kunskapen men inte bredden vilket kan försvåra processen med att använda verktyget. Med införande av förvaltningsmodell blir ansvaret tydligare för vem som ska tillse att resurs avsätts för att uppgiften konsekvensbedömning sker.

År 2023 uppmärksammade dataskyddsombudet att det fanns brister i stadens gemensamma arbete med konsekvensbedömningar. Det saknas en process och omhändertagande av dataskydd- och informationssäkerhetskrav vid konsekvensbedömningar. Behovet av att ha utsedd ledare för aktiviteten kvarstår. Under år 2024 deltog DSO och informationssäkerhetssamordnare vid konsekvensbedömning av stadens verktyg för att kommunicera krypterat/

skyddad med tjänsten ”Säkra meddelanden”. Work-shops leddes av SLK men när en av nyckelpersonerna där slutade, färdigställdes aldrig konsekvensbedömningen. Problemet som kvarstår i nuläget är en tjänst som inte är färdig utifrån analys, åtgärder och dokumentation. Verksamhetens krav har inte heller kunnat arbetas vidare med då det saknas ansvarig person att fråga hos leverantören, i det här fallet SLK.

Det uppstår ofta tidspress i det här arbetet då konsekvensbedömningar görs väldigt sent i framtagande av tjänster centralt. Värt att notera är att bolaget självt löser ut sina egna aktiviteter inom konsekvensbedömningar utan drabbas negativt vid det gemensamma arbetet.

2.4.4 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

2.4.5 DSO ger råd och rekommendationer till PUA

Konsekvensbedömningen som verktyg skapar bättre kravställningar redan i designstadiet och förenklar/förtydligar i avtal och kommunikation med leverantörer. Den gula markeringen synliggör bristen på gemensam process för stadens arbete med konsekvensbedömningar och som påverkar Familjebostäder negativt.

2.5 INDIVIDENS RÄTTIGHETER

2.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	Kan ej anges generellt då endast nekande registreras enligt Stadsarkivariens gallringsregler. Nekande radering 2
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	Kan ej anges då endast nekande registreras enligt Stadsarkivariens gallringsregler. Nekande radering 2

2.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen (artikel 12–22) ett antal rättigheter som på olika sätt ska garantera att den registrerade personen har insyn i hur dennes personuppgifter hanteras samt har en viss kontroll över personuppgiftsbehandlingen. Det är ett krav enligt förordningen att den verksamhet som enligt förordningen är att se som personuppgiftsansvarig – dvs. i stadens fall nämnder och bolag – tillgodoser rättigheterna i fråga.

Rättigheterna medför en rätt att ställa krav på att verksamheten vidtar vissa åtgärder, som exempelvis att lämna ut ett så kallat registerutdrag eller att rätta vissa uppgifter. (Radering, den så kallade ”rätten att bli glömd”, är sällan aktuell i någon större mån eftersom stadens verksamheter lyder under krav på bevarande till följd av offentlighetsprincipen.) Verksamheten har enligt dataskyddsförordningen artikel 12.3 en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran. (Notera dock att det finns undantagssituationer angivna i artikel 12.3, där fristen kan förlängas till mer än en månad.)

Dataskyddombudet har en roll i att granska efterlevnaden, identifiera brister samt ge råd och stöd hur processer och rutiner för att tillgodose rättigheterna bör utformas.

Om verksamheten inte klarar av att hantera en begäran från en registrerad person i enlighet med dataskyddsförordningen krav, kan det skada allmänhetens förtroende för hur staden hanterar personuppgifter. Det kan även leda till tillsynsärenden från Integritetsskyddsmyndighetens, IMY:s sida, med sanktioner som följd. Det är därför viktigt att PUA regelbundet ges en bild av i vilken mån

verksamheten klarar av att leva upp till regelverkets krav på att hantera begäran inom föreskriven tidsfrist.

2.5.3 Resultat

På Familjebostäder.com finns information om personuppgiftsbehandling och inhämtning av personuppgifter. Det finns även ett formulär för begäran om registerutdrag. Kundservice tar emot begäran om rättning vid namnbyte etc. Organisationen har också en portal för hyresgäster där man själv kan administrera sina uppgifter. Informationen till de anställda om behandling av personuppgifter är uppdaterad under året.

Under år 2024 har en handfull begäran från registrerade inkommit. Dessa har omhändertagits korrekt. Två nekande om radering har genomförts med hänvisning till att Familjebostäder har rättslig förpliktelse att spara informationen.

Detta kapitel omhändertar inte den brist om hanteringen av kakor som framkommit i kapitel 2.2.3 Resultat.

2.5.4 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

2.5.5 DSO ger råd och rekommendationer till PUA

DSO ger rådet att fortsätta arbeta transparent och att se över rutinerna om registerutdrag under 2025.

2.6 PERSONUPPGIFTSINCIDENTER

2.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	En utomstående eller medarbetare upptäcker incidenten.
Hur många personuppgiftsincidenter har dokumenterats?	8
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	0
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	0

2.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskyddsförordningen (artikel 4.12) ”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 en viktig och obligatorisk komponent bland dataskyddsförordningens olika verktyg för att åstadkomma en sund personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering.

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag från rapporteringsskyldigheten gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” (se artikel 33). Detta innebär att de flesta personuppgiftsincidenter ska rapporteras till IMY, inte senare än 72 timmar efter att verksamheten fått vetskap om incidenten. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter ska de berörda registrerade personerna, utan dröjsmål underrättas.

Dataskyddsförordningen delar alltså in personuppgiftsincidenter i tre kategorier: ingen rapportering, rapportering till IMY samt rapportering till de berörda personerna.

Bristande förmåga att rapportera personuppgiftsincidenter i tid kan leda till sanktioner från IMY. DSO:ns årsrapportering är därför avsedd att kartlägga detta, samtidigt som det finns möjlighet att redovisa vilka typer av personuppgiftsincidenter som inträffat, incidenternas allvarsgrad osv.

2.6.3 Resultat

Under år 2024 har åtta personuppgiftsincidenter uppmärksammats i organisationen. Det är samma antal som året innan men, omfattar en mer spridd typ av incidenter än tidigare. Två av incidenterna är orsakade av leverantör av tjänst. Brister uppstår i kommunikationen vid dessa båda tillfällen då den centrala incidentorganisationen inom staden inte fungerar och skapar en stor oro då det ofta blir ryktesspridning om vad som hänt och omfattning. Informationen och dess kanaler är i de båda fallen inte heller konsekvent utan sker i olika format och vägar.

2.6.4 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
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

2.6.5 DSO ger råd och rekommendationer till PUA

Styrelsen rekommenderas att dels ta fram en egen lokal organisation att omhänderta lessons learned. Det är en naturlig del av det förbättringsarbete som en mer mogen verksamhet kan ta nästa steg emot. Men, rekommendationen är också att ställa krav på att den centrala funktionen i staden omhändertar detta arbete bättre och blir mer transparent och förstår verksamhetens behov.

3 Genomförda granskningar under året

3.1 SAMMANFATTNING

Genomförda granskningar:

- *Implementation av AI och AI-tjänster*
- *Kontinuitetshantering*

3.2 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. Resultaten av granskningarna påverkar i stor utsträckning vilka beslut verksamheten kan fatta i fråga om dataskyddsåtgärder. För personuppgiftsansvarig är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under det gångna året och vad resultaten av granskningarna är.

3.3 GENOMFÖRDA GRANSKNINGAR OCH DERAS RESULTAT

3.3.1 Implementation av AI och AI-tjänster

Under år 2024 har flertalet AI-tjänster tillkommit inom IT-världen. Erbjudanden kommer titt som tätt och är av skiftande karaktär och seriositet. Utifrån integritetsperspektivet är det en komplicerad fråga där den registrerades behov av skydd behöver ställas mot en organisationens krav på digitalisering, effektivisering och utveckling.

Som en del av granskningen har diskussioner förts med projekt där AI kan vara av intresse att implementera. Tydligt är att en styrelse idag behöver ha en god insyn i riskarbetet och bestämma vilken riskaptit[2] organisationen ska ha genom styrelsens inriktningsbeslut. Med nya AI förordningen tillkommer också krav på leverantörer av dessa AI-tjänster och att de kan leverera de dokument som krävs för att Familjebostäder ska kunna göra rätt värderingar och analyser.

Ett gott steg i rätt riktning är arbetet med att ta fram egna lokala styrdokument utifrån informations-, dataskydds- och IT-säkerhetsperspektivet. Genom att börja hitta gemensamma vägar att låta informationssäkerheten styra genom krav på designen, kommer också individen att skyddas med rätt typ av säkerhet och projekten bli mer kostnadseffektiva.

En väg framåt i AI-införanden är att ta hjälp av de hyresgästföreningar som finns inom Familjebostäder. Att fråga dem om vad de tycker om en ny personuppgiftsbehandling kan ge en god vägledning om det är värt att arbeta vidare eller om en annan inriktning eller avgränsning behöver tas fram. Således

[2] Riskaptit- den nivå av risktagande som en organisation anser sig kunna acceptera innan den sätter in motåtgärder.

är inte endast tekniska lösningar viktiga vid införande av AI utan även mjuka värden måste beaktas och vägas in i analyserna.

3.3.2 Kontinuitetshantering

Under år 2024 har ett kontinuitetsprojekt startat inom Familjebostäder. Den granskning som planerades att genomföras av kontinuitetshanteringen under 2024 skjuts dock fram till år 2025. Anledningen är att projektet då har fortskridit än mer.

4 Risker inom dataskydd

4.1 SAMMANFATTNING

Relevanta risker inom verksamheten:

- Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (familjebostäders) objektförvaltning. (Ny)
- Ny teknik, t.ex. behandling av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation. (Ny)
- Tredjelandsöverföringar (Kvarstår)
- Osäker e-posthantering med personuppgifter (Kvarstår)

4.2 SYFTE

Verksamheten har ansvar för att göra vissa typer av riskanalyser, så som konsekvensbedömningar och informationsklassningar, men dessa ger inte en heltäckande bild av personuppgiftsriskerna i verksamheten. Dataskyddsombudet behöver som underlag för sin egen planering och sitt löpande arbete ha kontinuerlig överblick över dessa risker, i verksamhetens samtliga personuppgiftsbehandlingar. Exempelvis krävs en sådan överblick för att kunna välja ut vilka områden som bör granskas under det kommande året eller för att avgöra vilka råd som dataskyddsombudet behöver lämna till verksamheten om dataskyddsåtgärder som behöver vidtas.

Under år 2024 har en riskanalys genomförts tillsammans med informationssäkerhetssamordnaren för att hitta gemensamma åtgärder.

Risk beräknas utifrån RISK= Sannolikhet x Konsekvens

Sannolikhet (1 låg - 5 hög):
Låg risk - Inte trolig att inträffa
Hög risk - Kommer med all sannolikhet att inträffa

Konsekvens (1 liten - 5 stor):
Liten konsekvens - Ingen större påverkan
Stor konsekvens - Omfattande, dyrt kan ändra förutsättningarna dramatiskt

Riskvärde
Låg < 4 (riskerna skall bevakas)

Medel 5-14 (riskerna skall hanteras eller elimineras)

Hög > 15 (riskerna skall elimineras)

4.3 RESULTATET AV RISKKARTLÄGGNINGEN

4.3.1 Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (Familjebostäders) objektförvaltning

Som tidigare nämnt flera kapitel har det uppstått problem i införande av nya tjänster beroende på resursbrist hos central förvaltning. Detta påverkar implementation av nya gemensamma IT-tjänster och det systematiska arbetet som ska ske löpande i den egna lokala organisationen. En av de anledningar att exempelvis ”Säkra meddelanden” inte införts är då det saknas centralt utsedda ansvarsroller och åtgärder som ska införas inte följs upp eller återrapporteras att de genomförts.

	Hög > 15 (riskerna skall elimineras)
X	Medel 5-14 (riskerna skall hanteras eller elimineras)
	Låg < 4 (riskerna skall bevakas)

4.3.2 Ny teknik, t.ex. behandling av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation

Under år 2024 växte efterfrågan på AI och möjligheten att effektivisera arbetet. Då området är nytt och så även lagstiftningen behövs tydlig och transparent dokumentation när en sådan tjänst ska införas. Tyvärr brister ofta dokumentationen från leverantörerna och den som upphandlar verktyget behöver utbilda dem genom kravställning och möten.

Integritetsriskerna är stora då effektiviteten och möjligheten att ta fram ”smarta lösningar” tenderar att gå först i hela samhället. Mitt arbete som dataskyddsombud blir då i dessa införanden än mer viktigt att agera ombud och skydda de registrerades intressen.

En del i denna risk är också att nya funktioner införs i redan befintliga tjänster. Ett exempel på detta är en transkriberingstjänst vid digitala möten. Efter mötet är klart kommer direkt ett AI-genererat protokoll med sammanfattning, beslutspunkter och åtgärder. Det låter bra, men frågorna vi måste ställa oss då är vart sammanställdes informationen? Vem kan ta del av den? Hur känsligt blev materialet i det nya formatet? Osv. AI är ett oerhört bra och kraftfullt hjälpmedel som vi måste använda medvetet och till rätt saker.

X	Hög > 15 (riskerna skall elimineras)
	Medel 5-14 (riskerna skall hanteras eller elimineras)
	Låg < 4 (riskerna skall bevakas)

4.3.3 Tredjelandsöverföringar

Det nya inriktningsbeslutet från stadsledningskontoret som kom under hösten 2023 innebar en öppning för bolaget att använda leverantörer som använder sig av tredjelandsöverföringar. Förutsättningen är att verksamheten har en väl utformad exit-plan om överföringsmekanismen ”Data Privacy Framwork” ogiltigförklaras likt ”Privacy Shield” gjorde år 2020 och ”Safe Harbour” innan dess. I och med presidentvalet i november 2024, finns risk att den tidigare överenskommelsen med USA slås upp av den nytillträdande republikanske presidenten Donald Trumph. Flertalet leverantörer har därför börjat luta sig mot andra former av avtal för överföring till tredjeland som resultat av denna osäkra mekanism. Det i sig kräver att leverantörerna är mogna och har förberett sin dokumentation.

Flertalet leverantörer erbjuder idag endast molntjänster och de stora leverantörerna av sådana är amerikanskägda. Därav är detta en risk som behöver uppmärksammas extra.

X	Hög > 15 (riskerna skall elimineras)
	Medel 5-14 (riskerna skall hanteras eller elimineras)
	Låg < 4 (riskerna skall bevakas)

4.3.4 Risk 3 Osäker e-posthantering med personuppgifter

Varje personuppgift som ska hanteras måste behandlas säkert. När en personuppgift e-postas med någon av stadens leveranser sker själva överföringen krypterat, men är okrypterad i in- och utboxen. Det är också inte säkert att maila externt då exempelvis en medborgares adress inte kan kontrolleras på ett tillräckligt bra sätt.

Stadsledningskontoret har tagit fram en tjänst kallad ”Säkra meddelanden” eller ”TDialog”. Kvarstående aktivitet för verksamheten, är att se över och bedöma vad tjänsten kan användas till.

Jag som DSO kan inte rekommendera i dagsläget att tjänsten används efter att jag tagit del av analysmaterialet. Samtidigt är behovet kvarstående från verksamheten att möjligheten att e-posta personuppgifter säkert och krypterat.

När årsrapporten skrevs 2023 hade projektet med arbetet av dokumentationen för Säkra meddelanden startat på SLK. Detta för att kunna besvara de risker som framkommit inom de verksamheter som gjort ena konsekvensbedömningar och riskanalyser. Work-shops genomfördes sommaren 2024.

Rekommendationen kvarstår att inte använda tjänsten utan att analysmaterialet finns färdigt. Riskerna har inte besvarats av central förvaltning och informationsmängderna som ska skickas i det är så pass känsligt och skyddsvärt.

X	Hög > 15 (riskerna skall elimineras)
	Medel 5-14 (riskerna skall hanteras eller elimineras)
	Låg < 4 (riskerna skall bevakas)

4.4 DSO GER RÅD OCH REKOMMENDATIONER TILL PUA

Att ge råd om hur den centrala organisationen ska få mer resurs att utföra sitt arbete är svårt. Men, vi kan belysa utifrån Familjebostäders perspektiv att det blir svårt att arbeta effektivt när den brister och det tenderar att bygga flaskhalsar.

Som DSO rekommenderar jag att ni fortsätter vara nyfikna på ny teknik och våga satsa på den. Men, rekommendationen är att göra det med stor medvetenhet och arbeta efter den metod som finns framtagen för informationsklassning, riskanalys och konsekvensbedömning.

Risken att tredjelandsöverföringsproblematiken kommer att uppstå igen är sannolikt stor. Överföringsmekanismen bygger idag på en demokratisk presidentorder vilken kan rivas upp av den tillträdande republikanske presidenten under sin mandatperiod 2025-2029. Styrelsen rekommenderas att ta höjd för risken och bestämma aptiten för vad man är villig att riskera när man ingår nya avtal med leverantörer där överföringar till tredjeland sker. Rådet är också att ha en tydlig exitplan och genomlysa marknaden i förstahand inom Sverige och EU/EES.

Dataskyddsombudet rekommenderar att fortsätta efterfråga dokumentation och åtgärder för att kunna starta tjänsten säkra meddelanden.

5 Planerade granskningar under det nya verksamhetsåret

5.1 SAMMANFATTNING

Relevanta granskningsområden inom verksamheten:

- Kontinuitetshantering
- Personuppgiftsbiträde/ FAST2

5.2 SYFTE

Som nämnts tidigare är det granskande arbetet en av dataskyddsombudets viktigaste uppgifter. Eftersom dataskyddsombudet ofta har begränsat med tid, behöver granskningsplanen för det nya året utformas med eftertanke. Som en tumregel bör två-tre granskningar ses som en rimlig granskningsinsats under ett verksamhetsår. Granskningsområdena bör lämpligen väljas utifrån ett riskbaserat synsätt, det vill säga att fokus bör ligga på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Därigenom åstadkoms en röd tråd i dataskyddsarbetet från ett verksamhetsår till nästa samtidigt som de största riskerna elimineras eller åtminstone sänks till en mer acceptabel nivå.

5.3 PLANERADE GRANSKNINGAR

5.3.1 Granskning 1 Kontinuitetshantering

I händelse av avbrott i tjänster ska en kontinuitetsplan finnas för att tjänsterna ska kunna återupptas så snart som möjligt, om än eventuellt i begränsad funktion. Den ska innehålla en enkel plan och checklistor med:

- Reservrutin – Hur arbetar vi på alternativa sätt under en störning? Inklusive roller och ansvar.
- Återställningsrutin – Hur återställer vi den kritiska aktiviteten eller resursen efter en störning? Inklusive roller och ansvar.
- Återgångsrutin – Hur återgår vi till ordinarie arbetssätt när den kritiska aktiviteten eller resursen fungerar igen? Inklusive roller och ansvar.
- Nödvändiga kontaktuppgifter – Vilka kontaktuppgifter behövs för att kunna utföra uppgifterna? Vilka behöver informeras om läget, internt och externt?

Ändamålet att granska kontinuitetsplanerna är att ombesörja att dataskyddets krav på säkerhetsåtgärder och de registrerades intressen omhändertas även i kriser.

5.3.2 Granskning 2

Innan jag blev utnämnt till dataskyddsombud för Familjebostäder hade ett stort granskningsarbete inletts av flera organisationer gemensamt. Under 2025 har jag för avsikt att följa upp denna granskning och se över genomförda analyser.

6 Övrigt att rapportera

6.1 KLAGOMÅL

Familjebostäder har mottagit klagomål under 2024 genom tillsynsmyndigheten IMY, och som frågor via mail. Dessa har inte lett till djupare granskning av IMY men är en del av förbättringsarbetet och ger DSO en fingervisning var man ska börja granska arbetet internt.

6.2 INTERN ARBETSGRUPP

Under år 2025 behöver den arbetsgrupp som jobbade internt med dataskyddsfrågor under 2021, startas upp igen. Representanter i denna behöver vara utsedda utifrån förvaltningen av informationsmängderna. Syftet med en sådan grupp är att verksamheten kommer närmare Dataskyddsombudet och informationssäkerhetssamordnaren och ett utbyte av kunskap och behov flödar lättare. Arbetssättet har visat sig vara lyckat i andra verksamheter.

6.3 UTBILDNING

Familjebostäders informationssäkerhetssamordnare har under året hållit utbildning inom dataskydd och informationssäkerhet ”live” för medarbetare i organisationen.

De digitala obligatoriska utbildningarna behöver uppmärksammas av samtliga chefer för sina medarbetare.

Informationssäkerhets utbildning har 169 st. medarbetare av 337 st.
Dataskydds utbildning har endast 82 st. medarbetare av 337 st. genomfört, endast 24 %. En acceptabel nivå är ca 80 %.