Rapport

FB 2026/1

Dataskyddsombudets årsrapport 2025

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.

Den personuppgiftsansvariga, Familjebostäders styrelse, behöver ha god insikt i dataskyddsarbetet. Ett sätt att hålla sig informerad om risker och trender är den här årsrapporten.

Dataskyddsåret 2025 har varit fyllt av utmaningar men också möjligheter. En av nyheterna är att IMY, Integritetsskyddsmyndigheten, nu vill fokusera mer på vägledning än bestraffning. Det var med stor glädje vi mottog tydlig vägledning i både hur konsekvensbedömningar ska vara utformade och hur arbetet med AI-förordningen ska gå till.

Ett av de förbättringsområden jag vill belysa är utbildning och dataskyddskompetens inom organisationen. Det är ett lågt deltagande i de obligatoriska digitala utbildningarna och det avspeglar sig ibland annat det systematiska dataskyddsarbetet som är mycket personberoende. Det finns också en tendens att färre incidenter uppmärksammas av verksamheten.

En möjlighet som presenterads hösten 2025, är det nya förbättrade digitala verktyget för registerförteckningen. Det nuvarande utseendet har varit svårt att arbeta med för medarbetarna och det positiva är att leverantören lyssnat och gjort det mer användarvänligt. Projektet med att implementera detta sker under första kvartalet 2026. Som ett nästa steg behöver en intern arbetsgrupp för dataskydd och informationssäkerhet med representanter från hela verksamheten starta. På det sättet kan information lättare fångas upp och förmedlas till dataskyddsombud, informationssäkerhetsansvarig och till/ från medarbetarna.

En omvärldsbevakning från mig som DSO, är att tillsynsmyndigheten vill lägga mer fokus under 2026 på riskarbete inom dataskydd. Några av de riskområden som jag vill belysa i min årsrapport är:

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

Trots en tidvis omogen organisation när det kommer till dataskydd och informationssäkerhet, finns en ny inslagen väg med tydligare stöd från den nya Vd:n. Det är positivt och ger ny energi att nå ett mer systematiskt, mindre personberoende och mer riskmedvetet dataskyddsarbete.

Jessica Hillergård

Dataskyddsombud

Innehållsförteckning

1 Inledning

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

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

1.1 BESKRIVNING OCH FÖRKLARING AV GRANSKNINGSMETOD OCH RESULTAT

Dataskyddsombudet har granskat verksamhetens dataskyddsarbete utifrån sex obligatoriska områden. De sex områdena har identifierats genom en analys av kraven i GDPR om hur verksamheter bör arbeta systematiskt med dataskydd. Varje område innehåller ett antal kontrollfrågor som ger en bild av verksamhetens dataskyddsarbete. Dessa områden överensstämmer med de delar som enligt Integritetsskyddsmyndigheten, IMY, utgör grunden för en verksamhets systematiska och rättssäkra hantering av personuppgifter.

I rapporten används en riskmodell med fyra nivåer av risk. Modellen hjälper dataskyddsombudet att visa vilken bedömning hen gör av verksamhetens dataskyddsrisker utifrån de iakttagelser som gjorts i granskningen.

Risknivå	Beskrivning
Hög risk 	Iakttagelsen avser en brist som kan leda till betydande risker för de registrerades rättigheter och friheter. Bristen kräver omgående åtgärd och korrigering.
Medelhög risk 	Iakttagelsen avser en brist som kan leda till risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas skyndsamt, men kräver inte omedelbar korrigering.
Låg risk 	Iakttagelsen avser en brist som kan leda till mindre risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas, men kräver inte omedelbar korrigering.
Inget att anmärka 	Dataskyddsombudet har inga brister att rapportera avseende denna del som kräver åtgärder.

Notera att risken för att tilldelas en sanktion vid tillsyn är större desto högre risken är.

1.2 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
- Tekniska och organisatoriska säkerhetsåtgärder i samband med personuppgiftsbehandling[1]
- Konsekvensbedömningar
- Överföring till tredje land
- Individens rättigheter
- Personuppgiftsincidenter

Utöver dessa obligatoriska områden rapporteras även om de fördjupade granskningar som skett under föregående år samt planerade granskningsaktiviteter för år 2026. Ett specifikt kapitel om risker och

[1] I tidigare årsrapporter är denna punkt uppdelat i rubrikerna ”tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar” och ”styrdokument”

omvärldsbevakning är också prioriterat i rapporten för att underlätta beslut angående dataskyddsarbetet framåt för personuppgiftsansvarig.

2 Resultatsammanställning och centrala iakttagelser inom dataskyddsarbetet

2.1 REGISTERFÖRTECKNING

2.1.1 Syftet med området

I GDPR framkommer det att personuppgiftsansvariga (och personuppgiftsbiträden) ska föra ett register över sina personuppgifts-behandlingar. Registret brukar benämnas ”behandlingsregister” eller ”registerförteckning”. Registret ska finnas tillgängligt i elektronisk form och ska omfatta samtliga personuppgiftsbehandlingar som personuppgiftsansvarig utför. Det ska hållas uppdaterat vilket innebär att det ska uppdateras vid nya eller förändrade personuppgiftsbehandlingar.

Syftet med detta rapporteringsområde är att beskriva om verksamheten har ändamålsenliga rutiner som möjliggör att nya/förändrade personuppgifts-behandlingar registreras, huruvida personuppgiftsbehandlingar registreras/uppdateras såsom det krävs samt huruvida de uppgifter som är obligatoriska har besvarats kopplat till de registrerade personuppgiftsbehandlingarna.

2.1.2 Resultat

I årsrapporten från 2024 rekommenderades verksamheten att, vid den pågående kartläggningen av processägare och kontinuitetsprojekt, även lyfta in kontroll och uppdatering av registerförteckning i det arbetet. Syftet var att få systematik och minska personberoendet. Kontinuitetsarbetet har pågått under hela 2025 och är inte avslutat vid rapportens framställande. (Planeras vara klart Q2 2026.).

Registreringarna i registerförteckningen utgår från hanteringsanvisningen och dess processer och har fått utpekade ansvariga utifrån processägarskapet. Under 2025 har kontaktpersonerna uppdaterats. Rutin finns beskriven med ansvarsfördelning på Porten. Dock sker endast uppdateringar ad hoc av ISAM och DSO.

I kvartal 3 år 2025 släpptes en ny version av plattformen DraftIT som är det digitala verktyg stadens verksamheter använder för registerförteckningen. Familjebostäder har bestämt att under 2026 gå över till den nya plattformen då denna kommer bättre svara mot behovet organisationen har och kommer lösa delar med behörighetsproblematiken som finns i dagens verktyg.

2.1.3 Sammanfattning

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		147 personuppgiftsbehandlingar finns registrerade i DraftIT.

		I hanteringsanvisningen finns också kommentar om personuppgifter förekommer. I väntan på nya plattformen har prioritering lagts på hanteringsanvisningen- och process-inventering i en excellfil av verksamheten.
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		Registerförteckningen uppdateras inte löpande utan det sker ad hoc, rutin finns publicerad på Porten. Det har varit svårt för de ansvariga att uppdatera löpande p.g.a. behörighetstilldelningen i DraftIT. Det har också varit otydligt i organisationen vem som har ansvaret.
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		Veckovisa avstämningsmöten med ISAM/ arkivarie/ DSO med fast avstämningspunkt nya personuppgiftsbehandlingar, ger insyn i verksamheten. Då uppdateras också registerförteckningen om det behövts. Dock sker inte detta av verksamhetsansvariga.
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		De obligatoriska frågorna i formulären har besvarats men brister finns. Detta ska omhändertas i och med implementeringen av nya plattformen.

2.1.4 **DSO ger råd och rekommendationer till PUA**

Under år 2026 rekommenderas organisationen att fortsätta arbetet med övergången till den nya förbättrade digitala plattformen och att implementera de uppdateringar som uppmärksammats i samband med kontinuitetsarbetet och inventeringen i hanteringsanvisningen.

Organisationen rekommenderas också att ge de ansvariga en enklare utbildning och information om verktyget för att ett än mer systematiskt arbete ska kunna ske med registerförteckningen.

2.2 TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER

2.2.1 Syftet med området

Personuppgiftsansvarig ska tillse att personuppgifter skyddas med lämpliga säkerhetsåtgärder, detta för att till exempel undvika att obehöriga får tillgång till uppgifterna, att uppgifterna förloras eller förstörs.

Personuppgiftsansvarig behöver alltid bedöma vilka tekniska- och organisatoriska säkerhetsåtgärder som ska vidtas för de behandlingar som utförs. Till tekniska säkerhetsåtgärder räknas till exempel kryptering, behörighets-begränsning, pseudonymisering och säkerhetskopiering. Organisatoriska säkerhetsåtgärder avser till exempel interna riktlinjer och rutiner.

För att skapa förutsättningar för att skydda *all* information inom verksamheten och ha rätt nivå på skyddsåtgärder, ska verksamheten informationsklassa sin information. Stadens riktlinjer[2] för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA[3]. Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare.

Genom att använda arbetssättet i metodhandboken[4] värderas informationen utifrån konfidentialitet, riktighet och tillgänglighet. Verktyget KLASSA hjälper sedan till att ta fram tekniska och organisatoriska krav att ställa internt och mot leverantörer. Detta innefattar även bedömning och värdering av personuppgifter. Genom att genomför riskanalyser identifierar informationsägaren risker och väljer åtgärder för att hantera riskerna.

Den personuppgiftsansvariga måste kunna visa hur GDPR efterlevs och att det finns styrdokument och rutiner är en viktig del i detta. Det görs genom att det finns skriftliga, beslutade och kommunicerade styrdokument samt kända rutiner så att medarbetarna vet hur de ska agera avseende frågor som rör dataskydd.

Syftet med detta rapporteringsområde är att redogöra för huruvida DSO bedömer att det tas hänsyn till risker för den registrerade och om dessa beaktas i tillräcklig mån i genomförda informationsklassningar och riskanalyser samt att rätt bedömningen för både tekniska och organisatoriska åtgärder är gjorda. Vidare bedömer DSO också huruvida det finns tillräckligt mycket reglerat om dataskydd i styrdokument och rutiner samt om dessa är tillräckligt implementerade och kända.

2.2.2 Resultat

Familjebostäder är fortsatt en organisation som är i en relativt ung mognadsfas gällande informationssäkerhet och dataskydd. Det innebär att det finns ett stort personberoende för att rätt åtgärder och krav ställs när en IT-tjänst ska införas.

---

[2] https://intranat.stockholm.se/globalassets/stod-i-arbetet/rattsfragor-och-juridiskt-stod/informationssakerhet-i-staden/informationssakerhet/stadsledningskontoret/riktlinje-for-informationssakerhet.pdf (2026-01-05)
[3] KLASSA https://klassa.skr.se/ (2026-01-05)
[4] https://intranat.stockholm.se/globalassets/stod-i-arbetet/rattsfragor-och-juridiskt-stod/informationssakerhet-i-staden/informationssakerhet/stadsledningskontoret/handbok-for-informationsklassning-v.1.0.pdf (2026-01-05)

Rutiner finns men är inte fullt ut kända i hela organisationen. Med den nya Vd:n finns nu en tydligare styrning av området och det har fått den draghjälp som behövs att få det implementerat bredare i verksamheten. Ett tecken på det är kontinuitetsarbetet som pågått under 2025 och som färdigställs våren 2026.

2.2.2.1 Organisatoriska åtgärder

I rapporten för år 2024 angavs en större brist för cookie-policy och att den inte är korrekt. Detta ledde till en djupare granskning under 2025. Detta redovisas i eget kapitel. (3.3.2)

Under år 2025 har förklassningar skett och stämts av med DSO veckovis. En ny rutin för att ta fram personuppgiftsbiträdesavtal har testats under hösten och kommer fortsätta att förbättras under 2026. Det innebär att organisationen lättare ska kunna ställa rätt krav på leverantörer och arbeta aktivt med sina risker inom dataskydd.

2.2.2.2 Tekniska åtgärder

Familjebostäder är anslutna till CERT Stockholm. CERT Stockholm är stadens gemensamma funktion för att förebygga, upptäcka och hantera IT-säkerhetsincidenter. Cybersäkerheten stärks genom det med samordnad hotbild, rådgivning och omvärldsbevakning. Familjebostäder har ett bra IT-säkerhetsarbete och högt säkerhetstänk. Det är dock inte alltid så att dataskydd och informationssäkerhet får komma med i designarbetet utan kommer in senare i upphandlingar av IT-tjänster.

Utmaningen framöver kommer vara att fånga upp de AI:n som plötsligt implementeras i IT-tjänster och som skapar nya och oväntade personuppgiftsbehandlingar.

2.2.3 **Sammanfattning**

Fråga/kontroll	**Risk**	**Rekommendationer**
Efter ett antal stickprov på genomförda informationsklassningar, bedömer DSO att resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter?		De informationsklassningar som görs är bra och kompletta. Det som behöver bli bättre är att sprida kunskapen om arbetsmetodiken och ha ett mer talat ansvar i organisationen så att personberoendet att enskilda nyckelpersoner påminner om aktiviteten.
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		De styrande dokumenten finns publicerade på intranätet Porten. Dessa behöver uppdateras under 2026.

Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		De styrande dokumenten finns publicerade på intranätet Porten. Det behöver bli en ökad mognad inom organisationen och sprida kunskapen.

2.2.4 **DSO ger råd och rekommendationer till PUA**

Under 2026 behöver styrande dokument ses över och därefter kommuniceras tydligt i verksamheten så att beroendet av nyckelpersoner minskar för att åtgärder vidtas. Ett förslag är en utbildningsinsats där medarbetare får riktad information för sina behov på avdelningarnas informationsmöten. Ett annat förslag är att förtydliga ansvaret och uppmärksamma vilka aktiviteter som ska genomföras årligen för de medarbetare som har arbetsuppgiften.

2.3 KONSEKVENSBEDÖMNING AVSEENDE DATASKYDD

2.3.1 Syftet med området

En konsekvensbedömning avseende dataskydd krävs när personuppgiftsansvarig planerar att inleda en personuppgiftsbehandling som innebär hög risk för de registrerade. Huruvida en behandling innebär hög risk eller inte behöver personuppgiftsansvarig avgöra genom att genomföra en s.k. tröskelanalys.

En konsekvensbedömning ska vara genomförd för samtliga behandlingar som innebär hög risk, vilket innebär att personuppgiftsansvarig även behöver kontrollera huruvida denne utför befintliga behandlingar som innebär hög risk. Om högriskbehandlingar utfös för vilka en konsekvensbedömning inte har gjorts, behöver personuppgiftsansvarig genomföra en sådan.

Genom att genomföra en konsekvensbedömning kan personuppgiftsansvarig identifiera risker med en personuppgiftsbehandling, hantera riskerna genom åtgärder och rutiner samt påvisa ansvarsskyldighet. Genom konsekvens-bedömningar kan risker identifieras och förebyggas samt korrekta och relevanta skyddsåtgärder identifieras i kravställning på leverantörerna.

Syftet med detta rapporteringsområde är att rapportera huruvida verksamheten har ändamålsenliga rutiner som möjliggör att tröskelanalyser och konsekvensbedömningar genomförs, huruvida sådana genomförs när det krävs samt huruvida personuppgiftsansvarig har genomfört konsekvensbedömningar för de behandlingar som kräver det.

2.3.2 Resultat

I tidigare årsrapporter har det uppmärksammats att organisationen har rutiner och vägledning på intranätet Porten. Det finns en omognad i organisationen vilket leder till ett beroende av nyckelpersoner finns för att konsekvens-bedömningar ska utföras. Det leder till att det blir flaskhalsar som skulle kunna arbetas bort med tydligare förvaltningsorganisation och tydligare utpekat ansvar.

I Stockholm stad finns flera gemensamma IT-system och tjänster. Delmängder av Familjebostäders information finns i dessa system men kan ha en annan högre klassning än t.ex. en fackförvaltnings. Ett av de problem som uppmärksammats under flera år är när Familjebostäders medarbetare inte får vara med i designprocessen eller får ta del av information om tjänster efter att den införts eller inte längre kan påverkas. Det betyder att Familjebostäder inte kan uppfylla kraven som finns på organisationen som personuppgiftsansvarig och inte får kontroll på sina risker. Det saknas en process för vem som har ansvaret för att genomföra referens-konsekvensbedömningar i Staden och vilka som måste vara delaktiga.

2.3.3 Sammanfattning

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		När en förklassning genomförs besvaras också en enklare tröskelanalys. Denna kan dock bli bättre och mer anpassad till verksamheten med tydligare frågeställningar som vägleder lättare för medarbetarna.
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		Se ovan.
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		Ändamålsenlig och uppdaterad mall enligt IMY:s vägledning finns framtagen.
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		För de fall där Familjebostäder är ensamt ansvariga för personuppgiftsbehandlingar som kräver konsekvensbedömningar genomförs detta.
		Det saknas rutiner för hur centralt drivna konsekvensbedömningar ska ske för gemensamma IT-tjänster där det finns central förvaltning. Detta leder till att Familjebostäder inte kan agera korrekt utifrån dataskyddsförordningen och utföra sina egna åtgärder som personuppgiftsansvarig.
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		Familjebostäder har identifierat de personuppgiftsbehandlingar som kräver konsekvensbedömningar.
		När centrala och stadsgemensamma tjänster ska användas uppstår ibland nya personuppgiftsbehandlingar som kan kräva konsekvens-bedömningar. Om ISAM och DSO på bolaget inte deltar i centralt utförda

analysarbeten kan resultaten av dessa bli för generella och missa bolagsspecifika behov. Det krävs då större insatser av bolagets verksamhet att agera i efterhand, istället för att vara proaktiva.

2.3.4 DSO ger råd och rekommendationer till PUA

Under 2026 kan PUA med fördel se över mallen för förklassning och uppdatera den med en enklare tröskelanalys. Fortsatt behöver också det efterfrågas en stadsgemensam process för konsekvensbedömningar.

2.4 DEN REGISTRERADES RÄTTIGHETER

2.4.1 Syftet med området

Den registrerade har ett antal rättigheter enligt GDPR. Den registrerade kan bland annat begära tillgång (registerutdrag), rättelse eller radering. Den som är personuppgiftsansvarig har att tillmötesgå en begäran enligt de krav som finns i dataskyddsförordningen. (För registerutdrag säger GDPR 30 dagar och för övriga begäran skyndsamt.)

Syftet med detta rapporteringsområde är att kontrollera huruvida det finns ändamålsenliga mallar samt rutiner för besvarande av rättighetsbegäran, huruvida inkomna begäranden har hanterats inom den tidsram som finns att förhålla sig till samt huruvida svaren till de registrerade, baserat på ett antal stickprov, uppfyller lagkraven.

2.4.2 Resultat

På Familjebostäder.com finns information om personuppgiftsbehandling och inhämtning av personuppgifter. 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 finns publicerat på intranätet Porten.

2.4.3 Sammanfattning

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		Rutiner finns på intranätet Porten och på Familjebostäder.com finns förklaring hur man som registrerad kan utnyttja sina rättigheter.
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		Under året har 2 st. begäran från registrerade inkommit och dessa gallras efter ett år.
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		När en begäran inkommer löser organisationen ut en sådan fråga inom angiven tidsram.
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		Verksamheten uppfyller kraven enligt dataskyddsförordningen.

2.4.4 **DSO ger råd och rekommendationer till PUA**

Arbetet med att besvara och omhänderta begäran från registrerade fungerar bra. Organisationen är bra på att ge service. Rekommendationen är att se över mallar och texter enligt årlig aktivitet.

2.5 PERSONUPPGIFTSINCIDENTER

2.5.1 Syftet med området

Med begreppet personuppgiftsincident avses en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust, ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Om en inträffad personuppgiftsincident medför en risk/konsekvens för fysiska personers rättigheter och friheter ska den anmälas till Integritetsskydds-myndigheten, IMY, inom 72 timmar från att den upptäckts. Om personuppgiftsincidenten sannolikt leder till hög risk för de registrerade måste individen informeras utan onödigt dröjsmål. Om en personuppgiftsincident inte bedöms vara anmälningspliktig ska den dokumenteras. Det görs i verktyget IA.

Syftet med detta rapporteringsområde är att kontrollera huruvida det säkerställs att samtliga medarbetare har den kunskap som krävs om personuppgiftsincidenter, huruvida det finns ändamålsenliga rutiner för att hantera händelser som kan utgöra personuppgiftsincidenter och huruvida dessa rutiner följs.

2.5.2 Resultat

De incidenter som skett under året är betydligt färre än tidigare år, men det är nödvändigtvis inte dåligt. (Tidigare år har det varit 8 st. incidenter/ år) Det kan dock tyda på att det låga antalet medarbetare som genomgår utbildningen i dataskydd korrelerar med att färre incidenter uppmärksammas.

De incidenter som sker utreds ordentligt i samarbete med ISAM, IT och DSO. Det tas på stort allvar och lärdomar tas av IT när så behövs.

2.5.3 Sammanfattning

Fråga/kontroll	Risk	Rekommendationer
Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgifts-incident?		Samtliga medarbetare ska genomgå digital utbildning årligen i dataskydd. Dock är deltagandet lågt och kunskap är färskvara.
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgifts-incidenter? Följs dessa?		När Familjebostäder har incidenten i sina egna IT-tjänster löser verksamheten ut detta bra. Familjebostäder är ansluta till CERT Stockholm vilket betyder att ISAM får kontinuerliga rapporter om sårbarheter och brister.

		Svårigheter uppstår när det berör centrala IT-tjänster då informationsvägar inte är tydliga.
Hur många personuppgiftsincidenter har dokumenterats under året?		2
Hur många personuppgiftsincidenter har anmälts till IMY under året?		0

2.5.4 **DSO ger råd och rekommendationer till PUA**

Rådet som ges är att fokusera på att utbilda medarbetarna och fortsätta bygga kommunikationsvägarna med central förvaltning samt fortsätta den inslagna vägen med samarbete mellan IT, informationssäkerhet och dataskydd.

2.6 ÖVERFÖRING TILL TREDJE LAND

2.6.1 Syftet med området

För att säkerställa att den nivå av skydd för personuppgifter som ställs i GDPR inte undergrävs, får överföringar av personuppgifter till länder utanför EU/EES (tredje land) endast ske under särskilda förutsättningar. Det innebär att sådan överföring måste stödjas på antingen ett beslut från EU-kommissionen om att landet ifråga upprätthåller en adekvat skyddsnivå, att överföringen omfattas av en lämplig skyddsåtgärd eller i särskilda undantagsfall. Vidare behöver även kompletterade skyddsåtgärder, utöver de lämpliga skyddsåtgärderna, vidtas i vissa fall.[5]

Syftet med detta rapporteringsområde är att rapportera huruvida personuppgiftsansvarig har identifierat de tredjelandsöverföringar som utförs, huruvida personuppgiftsansvarig tillämpar överföringsverktyg på de tredjelands-överföringar som utförs och om nödvändiga bedömningar har gjorts avseende tredjelandsöverföringarna.

2.6.2 Resultat

I tidigare rapporter har tredjelandsöverföringar angetts som en risk. Nytt för 2025 årsrapport är att detta är ett separat kapitel.

Tredjelandsöverföringar är problematiska om de inte analyseras korrekt och att rätt avtal finns för underbiträden som leverantörer använder sig utav. Tredjelandsöverföringar är fortsatt omnämnt som en risk av den anledningen. Familjebostäder använder sig av tredjelandsöverföringar men omhändertar dessa korrekt genom analys och medvetenhet.

2.6.3 Sammanfattning

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelands-överföringar som utförs?		De tredjelandsöverföringar som finns är identifierade i verksamheten. Under 2026 med övergången till den nya plattformen i DraftIT kommer kartläggningen uppdateras.
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		När tredjelandsöverföringar har varit aktuella finns det omnämnt hur de omhändertagits i personuppgifts-biträdesavtalets instruktion.

[5] Europeiska dataskyddsstyrelsens (EDPB) Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överenstämmelsen med EU-nivån för skydd av personuppgifter, Version 2.0, Antagna den 18 juni 2021.

Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		När tredjelandsöverföring är aktuell efterfrågas TIA av leverantören/ personuppgiftsbiträdet. Denna bedöms sedan av ISAM och DSO som ger rekommendation om fortsatt progress eller inte med leverantören.

2.6.4 **DSO ger råd och rekommendationer till PUA**

Sannolikheten att tredjelandsöverföringar kommer öka, är stor i och med att flera IT-leverantörer flyttar sina tjänster från on-prem (egna servrar) till molntjänster. Under 2026 rekommenderas organisationen att arbeta aktivt med att informera utvalda medarbetare om tredjelandsöverföringar. Det finns också ett behov av att bestämma vilken riskaptit verksamheten har för tredjelandsöverföringar exempelvis genom en molnstrategi.

Det är en utmaning att upphandla tjänster och förvirring finns hos leverantörerna om vad som gäller. Därför är det viktigt att Familjebostäder blir en bra kravställare och kan fånga upp otydligheter med rätt frågeställningar till leverantörer.

3 Genomförda granskningar under året

3.1 SAMMANFATTNING

Genomförda granskningar:

- Granskning 1 Utbildning i dataskydd och informationssäkerhet
- Granskning 2 Information till den registrerade med fokus på externwebben

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 Granskning 1 utbildning i dataskydd och informationssäkerhet

En av de brister som identifierats i årsrapporten från 2024 och så även i årets, är behovet av nyckelpersoner för att aktiviteter ska ske med informationssäkerhet och dataskydd. I rapporten från 2024 framkommer att endast 24% av medarbetarna har genomgått den *obligatoriska årliga* utbildningen i dataskydd. För att dataskyddsarbetet ska bli mer systematiskt och mindre personberoende borde nivån vara 80% deltagande. Nyckelvärdet 80% är ett bra riktmärke då ex. föräldralediga och långtidsfrånvarande räknas bort.

2025 har siffran ökat till ca. 26% deltagande. (Då har siffror räknats med för både medarbetare som avslutat utbildningen och som registreras som pågående.)

3.3.2 Granskning 2 Information till den registrerade med fokus på externwebben

Ett av de områden som visat sig vara mest komplicerade att få kontroll över som personuppgiftsansvarig är informationen till den registrerade och då främst med fokus på cookies och andra typer av digitala spårare på publika hemsidor. Detta är en trend som man kan se hos många personuppgiftsansvariga i hela Sverige och inte endast hos Familjebostäder.

Familjebostäder har bra information till de registrerade genom policys och transparens på sin hemsida. Dock visar granskningen på några mindre förbättringsområden likt förtydligande i cookie-bannern där det ser ut att vara spårare från Google på hemsidan men dessa är avstängda osv. Även portalen för hyresgäster är medtagen i granskningen. Detaljerade brister och åtgärder är tidigare presenterat i egen föredragning internt.

3.4 DSO GER RÅD OCH REKOMMENDATIONER TILL PUA

Dataskyddsombudets rekommendation inför 2026 är att prioritera att *samtliga medarbetare och konsulter* genomför utbildningarna i dataskydd och informationssäkerhet. Kunskap är färskvara och det finns tydliga signaler att det är ett stort förbättringsområde och som gör att organisationen inte är så stark inom området.

I informationen till de registrerade och då främst digitala spårare rekommenderas Familjebostäder att omvärldsbevaka PTS (Post och Telestyrelsen) vägledningar om digitala spårare. Förändringar på området spås komma med den nya uppdaterade dataskyddsförordningen som bearbetas på EU kommissionen och ländernas tillsynsmyndigheter.

4 Risker inom dataskydd

4.1 SAMMANFATTNING

Prioriterade risker inom verksamheten:

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

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.

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. Under hösten 2025 har förbättringar skett men som i rapportens framtagande inte har hunnit med att implementeras. Risken fortsätter därmed att bevakas.

	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 startade efterfrågan på AI och möjligheten att effektivisera arbetet. År 2025 har det blivit än mer vardag och efterfrågan ökar konstant. 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 skpas ett AI-genererat protokoll med sammanfattning, beslutspunkter och åtgärder. Det låter bra, men frågorna vi måste ställa oss då är var sammanställdes informationen? Vem kan ta del av den? Hur känsligt blev materialet i det nya formatet? AI är ett oerhört bra och kraftfullt hjälpmedel men vi måste använda det riskmedvetet och till rätt saker.

AI-förordningen har också tillkommit under 2025 vilket ställer högre krav på den som upphandlar tjänster att ha kontroll på sina informationsflöden. Familjebostäder har tagit fram styrdokument som gäller AI. Dock kvarstår risken som hög då endast administrativa åtgärder täcker de åtgärder som behövs.

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. 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 har amerikanska ägare. Därav är detta en risk som behöver uppmärksammas extra.

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

4.3.4 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.

Rekommendationen kvarstår att inte använda tjänsten ”Säkra meddelanden” utan att analysmaterialet finns färdigt. Påtalade risker har inte besvarats av central förvaltning och informationsmängderna som ska hanteras i tjänsten kan vara både känsliga enliga dataskyddsförordningen och sekretessbelagda enligt offentlighets- och sekretesslagen.

X	Hög > 15 (riskerna skall elimineras)
	Medel 5-14 (riskerna skall hanteras eller elimineras)

	Låg < 4 (riskerna skall bevakas)

4.3.5 Lagringsytor utan kontroll

I den nya plattformen Nordic for Zoom (ersätter ZoomX) kommer det finnas möjlighet att dela dokument och skapa egna grupper fritt för samarbete både inom den egna organisationen och med andra. Till skillnad från i en gemensam mapp eller i en samarbetsyta på Sharepoint där administratörer med särskild behörighet kan följa upp och gallra information som inte längre är relevant så finns i Nordic for Zoom inte denna administrativa kontroll. Detta gör att kraven i dataskyddsförordningen om transparens (registerutdrag) och lagringsminimering inte kan efterlevas.

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 Stockholms stads 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 Familjebostäder 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. Den juridiska mekanism som tillåter överföring av personuppgifter till USA bygger idag på en presidentorder från en tidigare mandatperiod. Denna kan ogiltigförklaras av sittande eller tillkommande president. 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 i första hand undersöka tjänster inom Sverige och EU/EES.
- Dataskyddsombudet rekommenderar att fortsätta efterfråga dokumentation och åtgärder för att kunna starta tjänsten ”Säkra meddelanden”.
- Under arbetet med införande av Nordic for Zoom behöver risken med lagringsytor omhändertas. En rekommendation är att minst skapa en organisatorisk åtgärd med rutiner och förbud, om det inte går att tekniskt stänga av filöverföring, begränsa lagringstiden eller på annat sätt kontrollera ytorna.

5 Planerade granskningar under det nya verksamhetsåret

5.1 SAMMANFATTNING

Planerade granskningar kvarstår från 2025. Framflyttningen beror på att omprioriteringar behövts göras för att stötta verksamheten och att kontinuitetshanteringen inte färdigställts inom tidsperioden då granskningar genomförts.

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 personuppgiftsbiträdet Fast2**

Innan jag blev utnämnt till dataskyddsombud för Familjebostäder hade ett stort granskningsarbete inletts av flera organisationer gemensamt. Under 2026 har jag för avsikt att följa upp denna granskning och se över genomförda analyser.

6 Omvärldsbevakning

6.1 TILLSYNSMYNDIGHETEN OMORGANISERAS

Den 1.a januari 2026 omorganiserades Integritetskyddsmyndighetens, IMY:s, operativa del. Det har nu inrättats en avdelning för tillsyn och klagomål och en för vägledning, innovation och teknik. Syftet är att:

- stärka myndighetens förmåga att genomföra riskbaserad tillsyn,
- stärka myndighetens förmåga att ge tydlig och effektiv vägledning samt
- effektivisera myndighetens hantering av klagomål

Sannolikt kommer det här leda till fler tillsyner baserade på klagomål och som pressmeddelandet säger, genomföra riskbaserade granskningar av organisationer. Det innebär att organisationen behöver ha god kontroll över sina dataskyddsrisker och arbeta aktivt med dem.

6.2 KOMMANDE FÖRÄNDRINGAR AV DATASKYDDSFÖRORDNINGEN

Ett förslag har lämnats från Europakommissionen i november på förändringar i dataskyddslagstiftningarna inom EU. Förslaget syftar främst till att öka möjligheten för innovation och minska administrativa krav på mindre verksamheter. Förslaget var helt annorlunda än det som levererades som första utkast sex månader tidigare då fokus var att minska kravet på registerförteckning.

Analysen jag som DSO gör är, att områdets fokusområden svänger fort men tydligt är att en organisation fortsatt behöver vara en tydlig beställare till leverantörer av IT-tjänster och ha kontroll på sina legala- och informationssäkerhetskrav. Behovet av att göra riskanalyser och tänka till före och ta medvetna risker är en viktig fortsatt nyckelaktivitet inom dataskyddsarbetet.

6.3 TILLSYN AV MILJÖDATA INCIDENTEN

Under hösten 2025 skedde en större personuppgiftsincident hos leverantören Miljödata. Den berörde även delar av Stockholm stad då Stadsledningskontorets HR-avdelning hade beslutat att använda plattformen leverantören erbjöd. Familjebostäders medarbetare har inte varit aktuella i denna incident, men med anledning av IT-angreppet och den efterföljande läckan av personuppgifter har Integritetsskyddsmyndigheten, IMY, beslutat att inleda granskningar mot Miljödata samt två kommuner och en region som har använt företagets tjänster. (Göteborgs stad, Älmhults kommun och Region Västmanland)

Urvalet av de granskade aktörerna har gjorts baserat på typ av verksamhet som bedrivs och indikationer på risker då det var många aktörer berörda. Det finns i nuläget inga planer på ytterligare granskningar från IMY men det är heller inte uteslutet att det kommer att ske. Granskningarna kommer bli vägledande i hur en organisation måste agera innan en personuppgiftsbehandling sker.

6.4 ÖVRIGT

IMY har mer fokus på vägledning än bestraffning sedan ett år tillbaka. Det innebär att en organisation kan söka delaktighet i regulatoriska sandlådor där man testar sig fram till ex. ett nytt AI skulle kunna användas.

Under år 2025 lättades kamerabevakningslagen upp. Ett område som troligen kommer att granskas under 2026 av tillsynsmyndigheten är nog att efterlevnaden av lagen, dokumentationskrav och bedömningar.

7 Övrigt att rapportera

7.1 KLAGOMÅL

Integritetsskyddsmyndigheten har mottagit ett klagomål mot Familjebostäder under 2025. Detta är behandlat enligt rutin och var till följd av att den registrerade var missnöjd med det svar hen fått. IMY valde att endast informera om klagomålet och inledde ingen vidare granskning.

7.2 INTERN ARBETSGRUPP FÖR DATASKYDD OCH INFROAMTIONSSÄKERHET

Under år 2026 behöver en arbetsgrupp som jobbar internt med dataskyddsfrågor startas upp. Det har tidigare funnits men rann ut i sanden under pandemin. 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.