Stockholms stad

Bilaga 11

GDPR Årsrapport

År 2024

Bostadsförmedlingen AB

GDPR årsrapport
År 2024

Dnr: BOST 2024/1030
Utgivningsdatum: xxxx-xx-xx
Kontaktperson: Dani Cohen

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.

Bolaget har arbetat kontinuerligt med dataskyddsfrågor sedan Dataskyddsförordningen ikraftträdande. Särskilt vad gäller att kartlägga och dokumentera personuppgiftsbehandlingar, informera om bolagets personuppgiftsbehandlingar samt uppfylla de registrerades rättigheter. Under året har den rutin för genomgång och uppdatering av registerförteckningar som etablerades 2022 upprätthållits. Man har även påbörjat arbetet med att ytterligare förbättra förteckningen genom bättre mappning gentemot sina processer.

Bolaget har under året infört systematisk återkommande möten mellan DSO och verksamhet för att följa upp incidenter och hantera uppkomna frågor. Flera delar av verksamheten har också genomgått en riktad utbildning inom dataskydd. Bolaget visar en hög grad av mognad kring förståelse för dataskyddsarbetets vikt, samt omsorgen för hantering personuppgifter. När ny behandling eller förändrad behandling av personuppgifter diskuterats har dataskyddsombudet tillfrågats och en löpande dialog kring dataskyddsfrågor har funnits. Verksamheten har rutiner för att kunna klassificera information samt gör bedömningar av tekniska och organisatoriska åtgärder för dessa. Behov av konsekvensbedömningar har analyserats inom samtliga verksamheter och konsekvensbedömningar gjordes under 2023 och planeras följas upp under nästkommande år.
Även om vissa utvecklingsområden har identifierats är det min bedömning att bolaget inom dessa områden i huvudsak lever upp till de legala kraven i Dataskyddsförordningen.
För vissa områden som granskats inom ramen för denna rapport har särskilda brister identifierats. Dels gäller det brister i tecknande, innehåll och uppföljning av personuppgiftsbiträdesavtal där risker även finns för tredjelandsöverföringar. Risker finns även i arbete med incidenthantering vad gäller det systematiska arbetet och dokumenterad beredskap för att hantera dessa risker. I rapporten beskrivs även vissa brister i rutinen för registerutdrag vad gäller den information som lämnas till enskild när de begärt utdrag. Rapporten lyfter även en risk med tillgängligheten av rutiner för det systematiska dataskyddsarbetet för medarbetare.
Min rekommendation är att fortsätta arbeta med dessa risker under 2025, och utveckla det systematiska dataskyddsarbetet.

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?	65
Har nödvändiga uppdateringar gjorts?	Delvis
Bedöms registerförteckningen vara fullständig?	Ja
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

För att något ska gå att skydda måste det först vara synligt för verksamheten. 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).

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 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.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

65 personuppgiftsbehandlingar var registrerade vid utgången av verksamhetsåret 2024. Inventering av verksamhetens registerförteckningar har funnits som en årlig kontrollaktivitet i bolagets internkontrollplan sedan 2019. Inventeringen 2024 har skett hos respektive verksamhet.

DSO kontrollerar om nödvändiga uppdateringar gjorts

En registerförteckning är en pågående process. 2024 har enbart inneburit ett fåtal uppdateringar. Under året har verksamheten noterat att registerförteckningen behöver omarbetas till vissa delar. Det arbetet har inletts och beräknas vara klart under 2025.

DSO bedömer hur fullständig registerförteckningen är

Som beskrivs ovan behöver registerförteckningen omarbetas till vissa delar. Det arbetet har inletts och beräknas vara klart under 2025. Eftersom förståelse och upprättande av verksamhet är en pågående process bör ändå registerförteckningen i huvudsak anses vara fullständig, men uppdateringar och kontroll av processer samt rensning av system som inte längre används behöver göras.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

En rutin för hur personuppgiftsbehandlingar ska inventeras och uppdateras inom de olika delarna av linjeverksamheten etablerades under 2022 och ingår i internkontrollplanen. Samtliga verksamheter har rapporterat att de arbetat med registerförteckningen under året och gjort nödvändiga uppdateringar.

3.1.4 DSO anger hur allvarliga bristerna är på en skala

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

DSO bedömer att registerförteckningen huvudsakligen är fullständig, uppdaterad och håller god kvalitet även om ett större arbete nu pågår att förbättra den ytterligare. Rutiner för att arbeta med registerförteckningen hanteras och uppdateringar har skett under året. Brister kvarstår då registerförteckningen t.ex. behöver kontrollera att de system där personuppgifter hanteras är korrekt uppdaterad samt att processerna på ett tydligt sätt beskriver behandlingen.

3.1.5 DSO ger råd och rekommendationer till PUA

Arbetet med uppdatering av registerförteckning och förtydligande av processerna behöver fortsätta under året. Rutinen och hantering inom internkontrollplanen bör kvarstå även fortsättningsvis.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Ja, i huvudsak
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Ja, i huvudsak
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

Detta område syftar till att bolaget genom styrdokument ska kunna visa att det bedriver ett systematiskt dataskyddsarbete och att bolaget styr medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar PUA till medarbetarna 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 viktig princip i Dataskyddsförordningen är att PUA måste kunna visa att förordningens principer för behandling av personuppgifter efterlevs (artikel 5). Av det följer att viktiga arbetssätt och rutiner ska vara dokumenterade.

Rapporteringen inom detta rapporteringsområde är tvådelad; dels bedöms om verksamheten har 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 ska ses som en brist i förhållande till direkta lagkrav i dataskyddslagstiftningen. Men bristande styrning på grund av att lämplig styrande dokumentation saknas leder också

till exempel ofta till bristande kvalitet i hur verksamheten utför aktiviteter samt att verksamheten tar för mycket resurser i anspråk när återkommande situationer och arbetsuppgifter behöver hanteras och analyseras från grunden om och om igen.

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?

En uppsättning av grundläggande styrdokument/rutinbeskrivningar finns upprättade och beslutade enligt följande:

- Bostadsförmedlingens personuppgiftspolicy
- Bostadsförmedlingens personuppgiftspolicy för anställda, konsulter och arbetssökande
- Bostadsförmedlingens personuppgiftspolicy för fastighetsägare och samarbetspartners
- Bostadsförmedlingens personuppgiftspolicy för sociala medier
- Rutinbeskrivning att hantera den registrerades rättigheter och förfrågan om information till de registrerade
- Rutinbeskrivning hantering av personuppgifter på intranät, webb och sociala medier
- Skyddade personuppgifter – policy och handläggning
- Personuppgiftsincidentsrutin
- Rutin för processen konsekvensbedömning avseende dataskydd
- Mejlpolicy
- Lokal anvisning för informationssäkerhet

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

Ovanstående täcker det huvudsakliga behovet av styrdokument för dokumentering och efterlevnad av Dataskyddsförordningen. Bolaget följer stadens arbete med dataskydd som standard och rutiner kring inbyggt dataskydd genom lokala anvisningar finns på plats som arbetar med klassning och handlingsplaner för respektive objekt och system.

DSOs bedömer att de dokument som finns på plats är ändamålsenliga och håller i huvudsak lämplig kvalitet.
Rutinen för att hantera den registreras rättigheter och förfrågan om information till de registrerade behöver kompletteras. Ett sådant

arbete pågår på bolaget, men kvarstår till nästa verksamhetsår och utgjorde under året en egen punkt för särskild granskning.
Styrdokumentet för rapportering av incidenter håller hög kvalité men har en brist i relationen till den digitala utbildningen för medarbetare vad gäller rapportering av personuppgiftsincidenter och hur en sådan rapportering ska fungera.
Det saknas en plan/rutin för det kontinuerliga uppföljningsarbetet gällande konsekvensbedömning. Bristen för detta rör styrdokument, men beskrivs närmare under kapitel 3.4.

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

Incidenthanteringsrutinen har uppdaterats och utökats under året.
De styrdokument som finns sedan tidigare bedöms vara aktuella och hålla lämplig kvalitet. En brist är hanteringen av incidenter som har hög funktionalitet inom verksamheten men där eskalerings och hantering även behöver formaliseras genom rutinbeskrivningar.
Det saknas även en rutin för att bedöma behov av konsekvensbedömningar samt genomföra uppföljning av konsekvensbedömningar (se kapitel 3.4)

3.2.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att en incidenthanteringsrutin upprättas där information om hur man hanterar allvarliga incidenter beskrivs. Det för att kunna begränsa skador, känna till eskaleringsgrader och säkra spårbarhet i hantering av allvarligare incidenter.
DSO rekommenderar även att en rutin för systematiskt arbete med konsekvensbedömningar upprättas (se kapitel 3.4).

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?	33
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 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.

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

3.3.3 Resultat

Informationsklassning har helt eller delvis genomförts för 33 av 65 behandlingar. Klassningarna, som omfattar verksamhetssystemen Bostoc, Lime, Agda, webben, Husnet, Fastighetsägarportalen, samt Kuben har genomförts i enlighet med rutin och är därmed aktuella. De informationsklassningar som genomförts utgår från ett riskbaserat förhållningssätt och fokuserar på de verksamhetssystem som innehåller mycket personuppgifter. En handlingsplan för att åtgärda brister i organisatoriska och tekniska skyddsåtgärder finns framtagna i KLASSA. Dessa har överlämnats till respektive objektsansvarig och hanteras inom ramen för förvaltningen av systemet/processen eller särskilda projekt som leds av Utvecklingsavdelningen. Någon kontroll av huruvida lämpliga skyddsåtgärder faktiskt vidtagits med anledning av klassningen har inte genomförts i denna granskning.

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

Bolaget har en etablerad förvaltningsmodell i enlighet med stadens modell för strukturerad förvaltning av system och processer (PM3). Denna modell klargör styrning och ansvarsfördelning och utgör en förutsättning för att kunna arbeta systematiskt med informationssäkerhet. På bolaget finns utpekade mottagare av de handlingsplaner som upprättas efter genomförda informationsklassningar, vilket gör att det finns förutsättningar för att lämpliga skyddsåtgärder för personuppgifterna kan implementeras och upprätthållas.

Arbetet med att åtgärda identifierade risker i informationssäkerheten, utifrån genomförd klassning, pågår i flera förvaltningsobjekt.

Flera system hanteras av staden centralt och där verksamheten tar del av stadens lösningar och säkerhetsåtgärder. Vid införande av dessa behöver Bostadsförmedlingen som egen

personuppgiftsansvarig meddela och kontrollera att de säkerhetsåtgärder för informationen som finns är godtagbara.

3.3.5 DSO ger råd och rekommendationer till PUA

Bolaget skulle även behöva etablera en process föra att dokumentera godkännande och hantera system gemensamma för staden, men där bostadsförmedlingen även ensamt fungerar som personuppgiftsansvarig.

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?	Delvis

3.4.2 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). Det är viktigt att PUA genom årsrapporten får en uppdaterad bild av hur fullständig verksamhetens situation är i fråga om konsekvensbedömningar avseende dataskydd.

3.4.3 Resultat

Informationssäkerhetssamordnare har tidigare i samråd med berörda avdelningschefer och DSO genomfört fullständiga konsekvensbedömningar för de personuppgiftsbehandlingar som identifierats.

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

Konsekvensbedömningar genomfördes under 2023. Ytterligare en konsekvensbedömning gjordes för en behandling under 2024. Inga nya behandlingar eller större förändringar av personuppgifter har tillkommit under året. Ny typ av behandling av personuppgifter kan dock förekomma, främst när nya tekniska hjälpmedel tas in inom processer som tidigare bedömts.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Inga nya behandlingar eller större förändringar av personuppgifter har tillkommit under året.

Är de genomförda konsekvensbedömningarna aktuella?

Konsekvensbedömningarna har inte följts upp under året, men verksamheten planerar uppföljning under 2025. Detta då det planeras göras i samband med den större genomgången för registerförteckningen. Det saknas en dokumenterad plan för återkommande kontroller för konsekvensbedömning. Nuvarande konsekvensbedömningar kan dock fortfarande ses som aktuella eftersom de är relativt nya och någon ny eller ändrad behandling inte gjorts.

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

Ett större arbete med konsekvensbedömningar gjordes under 2023, och dessa konsekvensbedömningar kan fortfarande anses aktuella då det inte skett ny typ av personuppgiftsbehandling under året. Det

saknas dock rutiner för hur arbetet med konsekvensbedömningar ska göras och hur ofta dessa ska följas upp. Den bristen har redan noterats i samband med granskning av styrdokument – se kapitel 3.2.

3.4.5 DSO ger råd och rekommendationer till PUA

Det saknas tydlig skriftlig rutin för systematiskt arbete med konsekvensbedömningar (Se kapitel 3.2). Konsekvensbedömningar ska hållas aktuella och risker med personuppgiftsbehandlingen ska hanteras kontinuerligt. Riskanalyser behöver göras tillsammans med konsekvensbedömningarna och dokumenteras tydligt där risker för enskildas personuppgifter särskilt bedöms både för fri- och rättigheter men även för risker kring konfidentialitet, riktighet och tillgänglighet. DSO rekommenderar verksamheten att senast under 2025 göra en översyn över gjorde konsekvensbedömningar.
Dataskyddsombudets råd i samband med konsekvensbedömningar bör även dokumenteras särskilt.
DSO rekommenderar även att arbetet med konsekvensbedömningar dokumenteras i rutin för systematisk uppföljning, samt hur DSOs råd ska omhändertas.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	5
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	5

3.5.2 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 PUA tillgodoser rättigheterna i fråga.

Rättigheterna medför en rätt för den registrerade 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.

DSO 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 Dataskyddsförordningens krav, kan det skada allmänhetens förtroende för hur bolaget hanterar personuppgifter. Det kan även leda till tillsynsärenden från IMY, 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.

Under året genomfördes även en särskild granskning gällande rutinen för registerutdragen. Resultat för denna hanteras separat.

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

4 begäran om registerutdrag och 1 begäran om radering har inkommit under 2024. Samtliga rättigheter har hanterats inom föreskriven tidsfrist. Det finns en rutinbeskrivning för de registrerades rättigheter som redogör för de olika rättigheterna och hur handläggningen ska ske.

Rutinen för begäran om registerutdrag fungerar och följs. Förfrågan har hanterats i första hand av DSO och ISAM men det finns redundans på Kundservice vid semestrar eller liknande. Personuppgifter om kunder behandlas i huvudsak i två olika system, Bostoc och Lime, och de olika systemen behandlar olika kategorier av personuppgifter. Det saknas tekniska förutsättningar att skapa registerutdrag per automatik i verksamhetssystemen.

Möjligheter att radera uppgifter på begäran av den registrerade är begränsade med hänsyn till offentlighetsprincip och arkivlag. Det finns standardiserade svar gällande detta när begäran inkommer.

Vidare hanteras rättelse på begäran, direkt av Kundservice, förmedlingshandläggare eller DSO. Uppgifter kan också rättas av kunderna själva på ”Mina Sidor”.

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

Verksamheten har goda förutsättningar att hantera de registrerades rättigheter. Inkomna begäran hanteras inom tidsram, och prövas enligt laglig grund. Övriga rekommendationer och närmare kontroll av rutinen för registerutdrag görs i en egen granskning. Se kapitel 4.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Personuppgiftsincidenter upptäcks genom synpunkter/klagomål eller genom rapporter från anställda och biträden. Rapportering sker till närmsta chef och till DSO.
Hur många personuppgiftsincidenter har dokumenterats?	10
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	2
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	2

3.6.2 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.”

I en verksamhet kan förekomma många andra typer av incidenter, som inte involverar personuppgifter. Det är viktigt att hålla den saken i åtanke, så att årsrapporteringen inte omfattar annat än just personuppgiftsincidenter. Vidare är det en grundförutsättning för hanteringen av personuppgifter att incidenter över huvud taget upptäcks, samt att verksamheten förstår att hantera incidenter som rör personuppgifter på det särskilda sätt som Dataskyddsförordningen kräver.

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland Dataskyddsförordningen olika verktyg för att åstadkomma en sund personuppgiftshantering. Incidenthanteringen

består av två huvudsakliga moment – dokumentering respektive rapportering. Stadens mall för DSO:s årsrapport är avsedd att fokusera på rapporteringen.

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 och friheter, ska rapportering även ske till de berörda registrerade personerna, utan dröjsmål. 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:s sida. DSO:ns årsrapportering är därför avsedd att kartlägga detta, samtidigt som det finns möjlighet att redovisa vilka typer av personuppgiftsincidenter som inträffat, incidenternas allvarsgrad etc.

Notera att enligt Dataskyddsförordningen artikel 33.5 ska alla personuppgiftsincidenter dokumenteras, det vill säga även i de fall då incidenten inte ska rapporteras till IMY. Bristande dokumentering står i strid med Dataskyddsförordningen och leder även till problem med att ta fram korrekta siffror till årsrapporteringen avseende hur väl verksamheten lever upp till rapporteringsfristerna. Enligt artikel 33.5 är det ett krav att dokumentera omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden och bristande dokumentering är sanktionsgrundande.

3.6.3 Resultat

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

Verksamheten har en relativ god förmåga att hantera personuppgiftsincidenter. På högre nivå finns god kunskap kring

hantering av personuppgiftsincidenter. När incident rapporteras finns rutiner på plats för att snabbt kunna utreda, bedöma och rapportera incidenter till tillsynsmyndighet.
Utbildningar finns genom digitalt stöd. Risk är att rapporteringsvägarna kan vara osäkra då användaravtal och praktisk genomförande inte stämmer överens. Fördröjning har också inträffat vad gäller mindre allvarliga personuppgiftsincidenter.

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

Viss brist i kommunikation gällande rapporteringsvägar för personuppgiftsincidenter. Felaktig information eller avsaknad av information kan leda till fördröjningar för rapporter. Viss brist på förståelse för rapportering kan finnas ute i verksamhet.

3.6.5 DSO ger råd och rekommendationer till PUA

Personuppgiftsansvarig bör ge tydlig information om rapportering av personuppgiftsincidenter behöver kontinuerligt ges till samtliga anställda med förtydligande om rapporteringsvägar för att undvika försenade och/eller missade incidenter. Rapporteringsvägarna bör vara enkla och personoberoende. Staden arbetar just nu med att ta fram nya incidentrapporteringssystem. Bostadsförmedlingen bör tidigt överväga möjligheten att ingå i dessa eller se över behovet att ta fram egna.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- *Uppföljning av rätten till tillgång*
- *Personuppgiftsbiträdesavtal*

4.2 Syfte

En av DSOs 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 PUA är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under det gångna året och vad resultaten av granskningarna är

4.3 Genomförda granskningar och deras resultat

Granskning 1 - Uppföljning av rätten till tillgång

Bolaget har en rutin för utlämning enligt rätten till tillgång, skapande av registerutdrag. Antalet begärda sådana brukar under året vara relativt få. Som kommunalt bolag finns fler möjligheter att få tillgång till sina uppgifter, t.ex. via offentlighetsprincipen eller möjligheten att direkt se uppgifter i inloggat läge på t.ex. ”mina sidor”.
Sedan Dataskyddsförordningen trädde i kraft har rättspraxis utvecklat. Utifrån gällande praxis och beslut från bl.a. IMY har en gransnkning gjorts av nuvarande rutin.
Det finns idag goda rutiner för att få ut och leverera faktisk information om personuppgifter som hanteras av bostadsförmedling. Däremot visar nuvarande rutin vissa brister vad gäller enskildas rättigheter och information om syftet med behandlingen. Dataskyddsombudet rekommenderar bolaget att uppdatera rutinen för registerutlämning, för att bättre följa rådande rättspraxis.

	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

Granskning 2 - Personuppgiftsbiträdesavtal

Utifrån registret över behandling av personuppgifter har biträdesavtal följts upp när de tecknats direkt av Bostadsförmedlingen. Personuppgiftsbiträdesavtal har funnits för samtliga behandlingar. Rekommendation har varit att använda sig av stadens biträdesavtal. Det har dock inte alltid varit praktiskt möjligt för alla behandlingar. Avtalens innehåll och rutiner för tecknande av personuppgiftsbiträden har också följts upp. Instruktioner i personuppgiftsbiträdesavtalen har i varierande grad uppfyllt nödvändiga krav. Personuppgiftsansvarig behöver tydligt själva sätta upp de organisatoriska och tekniska åtgärder som är lämpligt för personuppgifterna. Dessa krav ska spegla det som kommer fram vid klassningen av personuppgifterna och vid riskanalyser och konsekvensbedömningar. När inte stadens mall används, t.ex. vid köp av licensierade molntjänster, behöver personuppgiftsbiträdesavtalet granskas för att se att de innehåller nödvändiga delar, instruktionerna överensstämmer med de krav som anses tillämpliga samt att eventuella underbiträden är korrekta. Bolaget skulle även behöva se över godkännande och tecknande av personuppgiftsbiträdesavtal så att instruktioner följder dessa principer. Risker finns att biträdesavtal godkänns där okontrollerad tredjelandsöverföring sker eller där avtalen inte följer vad som krävs enligt dataskyddsförordning.

I samband med granskning gjordes kontroll på två personuppgiftsbiträden. Granskningarna av biträden visade vid ett fall på ovana hos dessa att svara på uppföljningar trots att dessa är avtalade, vilket fördröjde uppföljning och gav begränsad information.

DSO rekommenderar personuppgiftsansvarig att ha rutiner för uppföljningar av personuppgiftsbiträden för att säkra att avtalade

instruktioner följs och att kravställda rutiner och åtgärder finns på plats. DSO rekommenderar även att tydlig instruktion/rutin finns för hur biträdesavtal tecknas i samband med inköp av system eller extern tjänst.

Bostadsförmedlingen ingår i upphandlingar gemensamt i staden, Enligt stadens modell innebär det att flertalet system upphandlas centralt av stadsledningskontoret och serviceförvaltningen där Bostadsförmedlingen ingår. Även vid sådana upphandlingar behöver ibland personuppgiftsbiträdesavtalet tas fram lokalt i verksamheten och korrekta säkerhetskrav ställas lokalt för den information som hanteras där.

	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

4.4 DSO ger råd och rekommendationer till PUA

Se råd och rekommendationer under respektive granskningsområde ovan under punkten 4.3.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- *Risker för tredjelandsöverföring*
- *Risk för incidenthantering*
- *Risker för rutiners tillgänglighet*

5.2 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. DSO 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 DSO behöver lämna till verksamheten om dataskyddsåtgärder som behöver vidtas.

Risk 1 Risker för tredjelandsöverföring

Som påpekats i samband med granskningen av personuppgiftsbiträden är det vid val och upprättande av personuppgiftsbiträdesavtal också viktigt att kontinuerligt följa upp avtal för att kontrollera att ingen olaglig tredjelandsöverföring sker. Efter Schrems II-domen innefattar tredjelandsöverföring att även ägande av bolag har betydelse för om det sker överföring till område utanför EU/EES. Det gör att personuppgiftsansvarig där personuppgifter överförs (t.ex. via cookies), biträden och underbiträden behöver granskas inte bara utifrån var data är placerad utan även bolagsstrukturer. Om överföring till tredje land baserar sig på standardavtalsklausuler (SCC) behöver en transfer impact assesment (TIA) dokumenteras.

	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

Risk 2 Risker för incidenthantering

Som anges i 3.6.2 är incidenthantering en viktig del i dataskyddsarbetet. För det har bolaget tagit fram en incidentrapporteringsrutin. Rapporteringsrutinens syfte är att hantera hur en incident ska rapporteras och initialt bedömas. Dock rekommenderas även att rutiner finns för hur kontinuitetsarbete och incidenter omedelbart omhändertas och dokumenteras. Även om bolaget i huvudsak visat goda kunskaper i hantering av incidenter, samt förmåga att omhänderta dessa i tid finns risker om rutiner inte finns tillgängliga eller arbetet är tydligt utformat. Utifall rutiner och känd dokumentation saknas riskerar förmågan vara personberoende. DSO rekommenderar dokumentation för incidenthantering, eskalering och loggföring. Det för att kunna bevaka och förhindra konsekvenser för registrerade och säkra att åtgärder görs i tid, samt att dessa dokumenteras vid rätt tillfälle.

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

Risk 3 Risker för rutiners tillgänglighet

Bolaget har flertalet rutiner för verksamhetens arbete. Det är viktigt att rutinerna också är tillgängliga för verksamheten när det behövs. Flertalet rutiner är kända för verksamheten främst genom utbildning och kunskaper hos ledning. Rutinerna behöver dock vara konstant lättillgängliga för alla berörda medarbetare, t.ex. genom publicering på intranät. Det är också viktigt att rutinerna och utbildningarna är konsekventa och inte skapar osäkerhet i hur personuppgifter ska hanteras. Verksamheten har svarat att risken ska omhändertas tidigt under 2025.

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

5.3 DSO ger råd och rekommendationer till PUA

Se råd och rekommendationer under respektive beskriven risk ovan under punkten 5.3.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Behörigheter för anställda som avslutar sin tjänst eller byter tjänst.*
- *Uppgiftsminimering i verksamhetssystem*
- *Cookie-hantering på bostadsförmedlingens hemsida.*

6.2 Syfte

Som nämnts ovan 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.

6.3 Planerade granskningar

Behörigheter för anställda som avslutar sin tjänst eller byter tjänst

Frågan om behörighetstilldelning och avslut av behörigheter i främst verksamhetssystem har tidigare lyfts som en risk av dataskyddsombudet. Granskningen syftar till att kontrollera rutiner för berörda system men även för tillgång till mappar och personuppgifter vid byte av tjänst och avdelningar inom bolaget. Granskningen kommer även särskilt kontrollera tillgänglighet för information om rutiner för detta enligt risk 3 i kapitel 5.2

Uppgiftsminimering i verksamhetssystem

Tidigare granskningar av Dataskyddsombud har visat på brister gällande uppgiftsminimering i verksamhetssystem. Uppföljning av den granskningen planeras under 2025.

Cookie-hantering

Bostadsförmedlingen har stor vikt av tillgänglighet på bostadsförmedlingens hemsida och mina sidor, där stora mängder uppgifter hanteras dagligen. Bolaget har särskilt arbetat med Cookie-hanteringen på bostadsförmedlingen under året. Granskningen syftar till att följa upp det arbetet, information som ges till användare samt att de cookies som används motsvarar de behov som Bostadsförmedlingen har. Granskningen tar också grund i den risk som uppmärksammas i rapporten gällande tredjelandsöverföring enligt risk 1 i kapitel 5.2.