Stockholms stad

Bilaga 2

Dataskyddsombudets årsrapport

2023

Bostadsförmedlingen i Stockholm AB

Dataskyddsombudets årsrapport
2023

Dnr: BOST 2023/146
Utgivningsdatum: 2024-02-01

1 Bakgrund

Enligt Dataskyddsförordningen är varje nämnd och bolagsstyrelse inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det är således bolagets styrelse som är personuppgiftsansvarig (”PUA”). Bolagsstyrelsen 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 har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är ett medel för styrelse att ta emot de råd och rekommendationer som DSO är skyldig att ge till ansvarig enligt Dataskyddsförordningen samt för att få insyn i vad DSOs granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att bolagsstyrelsen ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt.

Bolagsstyrelsen ska kunna *visa* att verksamheten efterlever Dataskyddsförordningen (den s.k. principen om ansvarsskyldighet). Årsrapporten är en mycket viktig del av denna dokumenteringsskyldighet. Årsrapporten är även ett medel för bolagsstyrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehåll

2 Sammanfattning

I egenskap av DSO lämnar jag följande årsrapport.

Bolaget har arbetat kontinuerligt med dataskyddsfrågor sedan Dataskyddsförordningens 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. Detta säkerställer god ordning för registerförteckningarna.

Bolaget har också under året färdigställt samtliga konsekvensbedömningar för de personuppgiftsbehandlingar där så bedömts nödvändigt.

Bolaget har fortsatt att inom förvaltningsorganisationen tillse att de handlingsplaner som upprättats som ett resultat av informationsklassningar av system och informationstillgångar omhändertas.

Bolaget har under året även utvecklat och implementerat loggning av åtkomst till personuppgifter i verksamhetssystemet Bostoc.

Inom ovanstående områden är det min bedömning att bolaget lever upp till de legala kraven i Dataskyddsförordningen.

För andra områden som granskats inom ramen för denna rapport har brister identifierats. Det handlar om styrande dokumentation kring behörighetshantering i verksamhetssystemen. Vidare finns alltjämt brister i uppfyllandet av de grundläggande principerna i Dataskyddsförordningens artikel 5 gällande lagringsminimering.

Min rekommendation är att fortsatt arbeta med ovanstående risker under 2024, för att öka kvaliteten i det löpande dataskyddsarbetet och tillse efterlevnaden av Dataskyddsförordningen.

3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som 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 samt personuppgiftsincidenter.

Nedan redogörs för bolagets status samt DSOs slutsatser och rekommendationer gällande de obligatoriska rapporteringsområdena efter DSOs genomförda uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	65
Har nödvändiga uppdateringar gjorts?	Ja, huvudsakligen.
Bedöms registerförteckningen vara fullständig?	Ja
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

Det följer av Dataskyddsförordningen (artikel 30) att stadens alla förvaltningar och bolag måste inventera alla personuppgifter som behandlas i verksamheten och dokumentera dem i en så kallad registerförteckning.

Registerförteckningen skapar 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. 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, då insatserna kan styras mot där de gör störst nytta.

Syftet med detta rapporteringsområde är således att rapportera till PUA hur väl verksamheten har lyckats inventera sina personuppgifter 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

65 personuppgiftsbehandlingar var registerförda vid utgången av verksamhetsåret 2023.

Inventering av verksamhetens registerförteckningar har funnits som en årlig kontrollaktivitet i bolagets internkontrollplan sedan 2019. Inventering och uppdatering av registerförteckningar har utförts av representanter för verksamheten till rapporteringen av tertialrapport 2.

En rutin för hur personuppgiftsbehandlingar ska inventeras och uppdateras inom de olika delarna av linjeverksamheten etablerades under 2022 och har efterlevts för 2023.

3.1.4 DSO anger hur allvarliga bristerna är på en skala

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

Det är DSOs bedömning att registerförteckningen huvudsakligen är fullständig, uppdaterad och att den håller god kvalitet. Rutiner för att arbetet med registerförteckningarna ska utföras i linjeverksamheten och att ansvaret för att personuppgiftsbehandlingarna registerförs och hålls uppdaterade finns på plats.

3.1.5 DSO ger råd och rekommendationer till PUA

Det bör även fortsättningsvis finnas utpekade aktiviteter i interkontrollplanen för att tillse att registerförteckningen ses över och hålls uppdaterad årligen.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Ja
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Ja
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Ja
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

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

Ovanstående täcker det huvudsakliga behovet av styrdokument för dokumentering och efterlevnad av Dataskyddsförordningen. Det saknas alltjämt viss dokumentation av vikt för dataskyddsarbetets styrning, såsom regelverk och rutiner kring inbyggt dataskydd och dataskydd som standard samt tekniska och organisatoriska säkerhetsåtgärder, se vidare nedan under punkten 3.2.4 om brister.

DSOs bedömning är att de dokument som finns på plats är ändamålsenliga och håller lämplig kvalitet.

3.2.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten

	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	**Inga brister av nämnvärd betydelse identifierade**

Inga nya styrdokument har tillkommit under året. De styrdokument som finns sedan tidigare bedöms vara aktuella och hålla lämplig kvalitet.

En identifierad brist som kvarstår sedan förra årets rapport är att det bör finnas en dokumenterad rutin för hur behörigheter i verksamhetssystemen beviljas och regelbundet följs upp och revideras.

3.2.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att tas fram en dokumenterad rutin för en regelbunden översyn av behörigheter i våra verksamhetssystem Bostoc, Lime och Fastighetsägarportalen, hur och vem som kan bevilja behörigheter och hur behörigheter ska ändras eller tas bort vid uppsägning eller byte av tjänst.

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 av 65 (informationsklassningarna omfattar dels personuppgiftsbehandlingarna som helhet, dels de system i vilka behandlarna helt eller delvis görs)
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 under 2022 och 2023 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 etablerat förvaltningsmodell i enlighet med stadens modell för strukturerad förvaltning av system och processer (PM3). Denna modell, som på ett tydligt sätt klargör styrning och ansvarsfördelning, 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.

3.3.5 DSO ger råd och rekommendationer till PUA

Bolaget har initialt valt att informationsklassa verksamhetssystemen. I och med att mognadsgraden i informationssäkerhetsarbetet ökar och förståelsen och kunskapen kring informationsklassningar förbättras är det DSOs rekommendation att fördela klassningarna utifrån informationsmängder och processer snarare än system. En sådan klassning är genomförd, där informationen i förmedlingsprocessen klassats, vilken hanteras i tre olika verksamhetssystem. Ingen rekommendation i övrigt.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Ja
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Ja
Är de genomförda bedömningarna aktuella?	Ja

3.4.2 Syfte

Konsekvensbedömningen 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

ISAM har i samråd med berörda avdelningschefer och DSO genomfört fullständiga konsekvensbedömningar för de 5 personuppgiftsbehandlingar som identifierades i föregående års tröskelanalys och som sannolikt kan leda till en hög risk för de registrerade ur ett integritetsperspektiv.

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**

Det är DSOs uppfattning att konsekvensbedömningarna skett i enlighet med Dataskyddsförordningen och stadens riktlinjer. Ingen av bedömningarna har resulterat i att begäran om samråd med IMY krävs.

3.4.5 DSO ger råd och rekommendationer till PUA

En konsekvensbedömning ska betraktas som ett levande dokument för att vidtagna åtgärder över tid ska medföra ett lämpligt skydd. Om någon av de behandlingar som nu genomgått en konsekvensbedömning ändras på ett sätt som förändrar risknivån ska en ny konsekvensbedömning genomföras. Ingen rekommendation i övrigt.

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 begäran om tillgång 6 begäran om radering
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	Samtliga

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.

3.5.3 Resultat

5 begäran om registerutdrag och 6 begäran om radering har inkommit under 2023. 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 hanteras i första hand av DSO men det finns redundans på Kundservice vid semestrar eller liknande. Personuppgifter om kunder behandlas 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 offentlighetsprincipen. 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 vad avser rätten till tillgång (registerutdrag) i enlighet med Dataskyddsförordningen. Det finns skriftliga rutiner för

hanteringen av rättigheterna som DSO bedömer efterlevs och fungerar.

Det saknas alltjämt möjligheter att få ut automatiserade registerutdrag från verksamhetssystemen Bostoc och Lime, vilket innebär att det krävs ett stort mått av manuell hantering att upprätta ett registerutdrag. Det ökar arbetsinsatsen och risker för manuella fel. Med tanke på att det är relativt få förfrågningar per år, och förfrågningarna har minskat från föregående år, är detta dock ingenting som kräver åtgärd i nuläget.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Personuppgiftsincidenter rapporteras till DSO genom funktion.dataskyddsombud@bostad.stockholm.se och genom bolagets ärendehanteringssystem Lime.
Hur många personuppgiftsincidenter har dokumenterats?	2
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	0
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Ej relevant

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.”

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland Dataskyddsförordningens olika verktyg för att åstadkomma en sund personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering.

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag från rapporteringsskyldigheten

gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” (se artikel 33). Detta innebär att de flesta personuppgiftsincidenter ska rapporteras till IMY, inte senare än 72 timmar efter att verksamheten fått vetskap om incidenten. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter 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. Denna årsrapportering är därför avsedd att kartlägga detta och samtidigt redovisa vilka typer av personuppgiftsincidenter som inträffat, incidenternas allvarsgrad etc.

Alla personuppgiftsincidenter ska 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

2 personuppgiftsincidenter har dokumenterats under året. Ingen av de dokumenterade incidenterna har bedömts vara så allvarlig att den rapporterats till IMY.

Felaktig hantering av intyg och/eller kreditupplysning i verksamhetssystemen har meddelats DSO 3 ggr under året. Ingen av dessa har dock bedömts så allvarlig att det dokumenterats som en personuppgiftsincident. Det finns en dokumenterad rutin för hur detta ska hanteras på bolaget när det inträffar. Arbetet med att implementera en integration mot bolagets leverantör av kreditupplysningar är nu slutfört, vilket innebär att

kreditupplysningar per automatik sparas i rätt kundärende. Detta har lett till en signifikant minskning av denna typ av incidenter.

3.6.4 DSO anger hur allvarliga bristerna är på en skala

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

Det finns en dokumenterad incidentrutin som följer stadens rutin för personuppgiftsincidenter. Det finns också en lokal rutin för hantering av intyg och/eller kreditupplysningar som av misstag laddas upp i fel kunds ärende. DSOs bedömning är att det finns relativt god kunskap och förståelse i organisationen för vad en personuppgiftsincident är och att detta bör meddelas till DSO när det inträffar.

Tidigare dokumenterade brister är huvudsakligen åtgärdade. Det finns numera en integration på plats mellan verksamhetssystemen och bolagets leverantör av kreditupplysningar, vilken innebär att inhämtad kreditupplysning automatiskt sparas i kundärendet. Detta utesluter risken för felaktigt sparade kreditupplysningar i systemet. Därtill speglas inte längre kreditupplysningar och intyg eller övriga handlingar på ”Mina Sidor” vilket gör att obehöriga inte har tillgång till de handlingar som av misstag sparats i fel kundärende.

3.6.5 DSO ger råd och rekommendationer till PUA

Inga rekommendationer.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Personuppgiftsincidenter till följd av manuell hantering av intyg och kreditupplysningar
- Lagringsminimering
- Behörighetshantering och behörighetsstruktur

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 - Personuppgiftsincidenter till följd av manuell hantering av intyg och kreditupplysningar

Bolaget har under en längre tid, pga manuell hantering av uppladdning av kreditupplysningar och övriga intyg i verksamhetssystemet Bostoc, haft återkommande personuppgiftsincidenter som beror på att dokument av misstag laddas upp i fel kundärende. Arbete har pågått för att åtgärda dessa brister. Under året har en integration mellan verksamhetssystemet och upphandlad leverantör av informationsdatabastjänster kommit på plats vilket automatiserar hanteringen av kreditupplysningar. Det har fått till följd att uppladdning av kreditupplysningar i fel kundärende inte längre sker.

Hanteringen av inkomna intyg (dvs. ej kreditupplysningar) är oförändrat. Det pågår dock utvecklingsprojekt på bolaget som syftar till att bostadssökande själva ska kunna ladda upp sina intyg via ”Mina Sidor”. Detta arbete kan innebära att felaktigt sparade intyg helt försvinner. Det pågår också ett arbete med att minimera den manuella hanteringen av intyg för handläggarna genom att inkomna intyg konverteras till pdf och skickas till Bostoc via Lime. På så sätt behöver handläggaren inte spara ned intyg på gruppdisk.

Det kan också tilläggas att kunder inte längre kan se uppladdade intyg på ”Mina Sidor” i inloggat läge. Detta har tagits bort som en åtgärd för att öka skyddet för personuppgifter så länge som lösenordsinloggning till ”Mina Sidor” är möjligt. På så sätt har risken för dessa typer av personuppgiftsincident avsevärt minskat, eftersom kunder inte kan se felaktigt uppladdade dokument.

Det är DSOs bedömning att hanteringen vid inhämtning av kreditupplysning och intyg hanteras på ett tillfredsställande sätt.

	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**

Granskning 2 – Lagringsminimering

En brist som rapporterades i förra årets rapport var bristande uppfyllande av principen om lagringsminimering.

Den 14 november 2022 beslutade Stadsarkivet om nytt verksamhetsspecifikt gallringsbeslut för bolagets information i verksamhetssystemen Bostoc och Lime (SSA 2022:15). Tidigare gallringsbeslut har föreskrivit ett huvudsakligt bevarande av informationen, vilket inneburit att mycket personuppgifter ligger sparade i verksamhetssystemen. Det nya gallringsbeslutet innebär att förutsättningarna för att kunna gallra information (inbegripande personuppgifter) numera finns på plats.

Granskning av efterlevnaden av gallringsbeslutet har visat att det ännu inte fullt ut tillämpas. Viss gallring sker, men det saknas automatiserade processer i verksamhetssystemen för detta, och vissa handlingar och uppgifter sparas längre än den frist som föreskrivs i beslutet.

Därtill gäller att verksamheten, för att fullt ut efterleva principen om lagringsminimering, behöver särskilja uppgifter som inte längre är aktuella för förmedlingsverksamheten, och som bevaras pga skyldigheten att bevara allmänna handlingar, från det aktiva registret. För det skulle krävas någon typ av mellanlagring, alternativt att inaktiva uppgifter tas bort från verksamhetssystemen sedan de skickats till Stadsarkivets e-arkiv och sparas endast i arkivsyfte för arkiveringsändamål. Detta sker inte idag.

	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 3 – Behörighetshantering och behörighetsstruktur

En identifierad brist i förra årsrapporten var styrdokument för behörighetshanteringen i verksamhetssystemen. Det ska finnas dokumenterade rutiner för hur behörigheter i verksamhetssystemen tilldelas, ändras, kontrolleras och avslutas. Därtill ska det vara tydligt vilken typ av behörighet som en medarbetare ska ha utifrån arbetsuppgifter och ansvarsområde, med principen minsta möjliga behörighet.

Verksamhetssystemet ska också ha tekniska förutsättningar för att begränsa så att handläggare exempelvis endast kan se ärenden som tilldelats deras enhet eller att handläggare inte kan komma åt arkiverade ärenden.

DSO har granskat detta område och kan konstatera att bristen kvarstår. Ingen dokumentation finns på plats och verksamhetssystemens förmåga att tekniskt begränsa användares

tillgång till personuppgifter utifrån principen minsta möjliga behörighet är alltjämt bristfällig.

	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

4.4 DSOs 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:

- Bristande uppfyllande av principen om lagringsminimering
- Efterlevnad av implementering av lämpliga tekniska säkerhetsåtgärder (art 32 Dataskyddsförordningen)

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.

5.3 Resultatet av riskkartläggningen

Risk 1 - Bristande uppfyllande av principen om lagringsminimering

Se avsnitt 4.3 ovan. Granskning av efterlevnaden av principen om lagringsminimering visar att brister alltjämt kvarstår.

	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 rekommenderar att PUA tillser att SSA 2022:15 tillämpas i sin helhet för samtliga uppgifter och handlingar i verksamheten för att säkerställa att principen om lagringsminimering av personuppgifter uppfylls. DSO rekommenderar också att avregistrerade kunders personuppgifter avskiljs från verksamhetssystemet för att begränsa åtkomsten till dessa och säkerställa en säker hantering av uppgifter som endast behandlas för arkiveringsändamål.

Risk 2 - Lämpliga tekniska säkerhetsåtgärder (art 32 Dataskyddsförordningen)

En risk som identifierades i förra årets rapport är bristande lämpliga tekniska säkerhetsåtgärder avseende inloggningsmetod till ”Mina Sidor”. Denna risk har åtgärdats genom att intyg och kreditupplysningar och andra dokument hänförliga till en bostadssökande inte längre finns tillgängliga på ”Mina Sidor”. På så sätt finns inte längre åtkomst till extra skyddsvärda personuppgifter via lösenordsinloggning.

På bolaget pågår olika utvecklingsprojekt med syfte att förenkla förmedlingsprocessen för de bostadssökande och att kommunikationen med de bostadssökande huvudsakligen ska ske via ”Mina Sidor”. För att det ska vara ändamålsenligt och ge effektivitetsvinster krävs att intyg och andra handlingar som är nödvändiga för prövningen av en bostadssökande inhämtas och sparas på ”Mina Sidor”. För att den hanteringen ska vara enhetlig

med dataskyddslagstiftningen och informationssäkerhetsstandard krävs flerfaktorsautentisering till ”Mina Sidor”, dvs. e-legitimation.

DSO rekommenderar att det i projekten säkerställs att inloggningsmetoden till ”Mina Sidor” bestäms med beaktande av risken för de registrerades integritet och personuppgifternas skyddsvärde.

5.4 DSOs 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:

- *Rätten till tillgång*
- *Personuppgiftsbiträdesavtal*

6.2 Syfte

Som nämnts ovan är det granskande arbetet en av DSOs viktigaste uppgifter. Granskningsarbetet behöver struktureras och planeras så att det kan genomföras under året samt att det sker utifrån ett riskbaserat synsätt, dvs. att fokus ligger på områden där verksamhetens mest relevanta risker har identifierats utifrån denna eller tidigare årsrapporter. 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

Granskning 1

Granskning av bolagets rutin för framtagande och utlämnande av registerutdrag, såväl för kunder, anställda och arbetssökande.

Granskning 2

Genomgång av bolagets befintliga personuppgiftsbiträdesavtal för att tillse att de är gällande och uppdaterade. Även granskning om det saknas personuppgiftsbiträdesavtal för huvudsakliga leverantörer som behandlar personuppgifter för bolagets räkning.