Stockholms stad

Bilaga 2

Dataskyddsombudets årsrapport

2021

Bostadsförmedlingen i Stockholm AB

Dataskyddsombudets årsrapport
2021

Dnr: BOST 2021/143
Utgivningsdatum: 2022-02-03
Kontaktperson: Lina Jurbrant

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 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 således 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.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att bolagsstyrelse ska kunna *visa* att verksamheten efterlever Dataskyddsförordningen. 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.

Sedan Dataskyddsförordningens ikraftträdande har kunskapen om respekten för den enskildes integritet ökat och dataskyddsarbetet har blivit en viktig verksamhetsfråga, både vad gäller effektiva arbetsprocesser som förtroendet från kunder och medborgare. Bolaget har arbetat kontinuerligt sedan 2018 med att kartlägga och dokumentera personuppgiftsbehandlingar, informera de registrerade och uppfylla de registrerades rättigheter vad gäller exempelvis tillgång till personuppgifter (registerutdrag).

Under året har verksamheten arbetat med rutiner och säkerhetslösningar för behandlingen av skyddade personuppgifter. Detta har avsevärt förbättrat hanteringen av dessa personuppgifter och ökat medvetenheten kring riskerna.

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

För andra områden som granskats inom ramen för denna rapport har brister identifierats. Det handlar främst om genomförandet av s.k. konsekvensbedömningar, styrande dokumentation kring tekniska och organisatoriska säkerhetsåtgärder samt inbyggt dataskydd och dataskydd som standard, rutiner för informationsklassning av personuppgifter och omhändertagande av handlingsplaner till följd av informationsklassningar. Vidare finns brister i uppfyllandet av de grundläggande principerna i Dataskyddsförordningens artikel 5 gällande lagringsminimering och uppgiftsminimering.

Min rekommendation är att arbeta med ovanstående risker under 2022, för att öka kvaliteten i det löpande dataskyddsarbetet och tillse efterlevnaden av Dataskyddsförordningen.

Lina Jurbrant
Dataskyddsombud

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?	60
Har nödvändiga uppdateringar gjorts?	Ja
Bedöms registerförteckningen vara fullständig?	Ja
Har verksamheten lämpliga rutiner för registerföring?	Delvis

3.1.2 Syfte

Det följer 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.

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, 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

60 personuppgiftsbehandlingar var registerförda vid utgången av verksamhetsåret 2021.

Inventering och uppdatering av registerförteckningarna har skett med regelbundenhet sedan de upprättades i samband med Dataskyddsförordningens ikraftträdande 2018. Inventering av verksamhetens registerförteckningar har funnits som en kontrollaktivitet i bolagets internkontrollplan under 2019, 2020 och 2021. Inventering och uppdatering av registerförteckningar har utförts av DSO i samverkan med representanter för verksamheten under första halvåret av 2021.

Det saknas fastställda rutiner för hur personuppgiftsbehandlingar ska inventeras och uppdateras inom de olika delarna av linjeverksamheten.

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

Det är DSOs bedömning att registerförteckningen huvudsakligen är fullständig och att den håller god kvalitet. Den samlade riskbedömningen bygger på att det saknas fastställda rutiner för hur arbetet med registerförteckningarna ska utföras i linjeverksamheten och att ansvaret för att personuppgiftsbehandlingarna registerförs

och hålls uppdaterade i praktiken har landat hos DSO. DSO ska i sin tur inventera och kontrollera kvaliteten på registerförteckningen, varför det inte är lämpligt att DSO utför själva registreringen. Därtill är det en risk att nya behandlingar förbigås eller nödvändiga uppdateringar inte sker när det saknas en intern struktur för att hålla en korrekt, komplett och uppdaterad registerförteckning.

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. Verksamheten bör, tillsammans med DSO, ta fram och fastställa interna rutiner för arbetet med registerförteckningen. Det bör av PUA finnas utpekat ansvariga för registerförteckningen på respektive avdelning, exempelvis enhets- eller avdelningschef. Dessa bör vid särskild utsedd tidpunkt under året se över registerförteckningarna. Detta ska, vid behov, ske i samråd med DSO.

3.2 Styrdokument

3.2.1 Sammanfattning

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

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
- 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

Ovanstående täcker väsentligen det grundläggande behovet av styrdokument för dokumentering och efterlevnad av Dataskyddsförordningen. Det saknas 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. Vissa av dokumentet behöver uppdateras, exempelvis ”Skyddade personuppgifter – policy och handläggning”.

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

Det saknas styrdokument gällande inbyggt dataskydd och dataskydd som standard. Med detta finns en ökad risk för att system och digitala tjänster utvecklas utan att ta hänsyn till de grundläggande principerna i Dataskyddsförordningen och utan att ta till vara på tekniska lösningar som ser till att dataskyddsprinciperna efterlevs, såsom exempelvis minimering av fritextfält, minimering av insamling av personuppgifter eller att systemet inte tillåter manuell hantering av uppladdning av dokument.

Ytterligare en identifierad brist är att det saknas dokumentation som berör tekniska och organisatoriska säkerhetsåtgärder som krävs för de olika personuppgiftsbehandlingarna som bolaget gör. Sådana rutiner ska exempelvis föreskriva att informationsklassning ska genomföras för alla personuppgiftsbehandlingar vid viss tidpunkt (varje eller vartannat år), rollbeskrivningar med ansvarsfördelning för olika informationstillgångar och personuppgiftsbehandlingar samt exempelvis förvaltningsplaner eller handlingsplaner genom vilken informationsägaren årligen ställer krav på tekniska åtgärder till systemförvaltaren. Det bör också finnas en dokumenterad rutin för hur behörigheter i verksamhetssystemen beviljas och regelbundet följs upp och revideras.

Slutligen är det en risk att det inte för samtliga styrdokument finns utpekade ansvariga. Detta kan leda till att dokumenten inte uppdateras och att de inte sprids tillräckligt i organisationen.

3.2.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att styrdokumenten får tydliga ägare och att de, i samråd med DSO, ses över en gång årligen, exempelvis till tertialrapport 2.

DSO rekommenderar också att avdelningen för Digitala Tjänster, Utvecklingsavdelningen och Förmedlingsavdelningen, i samråd med DSO, ser över behovet av styrdokument avseende hur verksamheten ska hantera inbyggt dataskydd och dataskydd som standard för utveckling av befintliga och nya verksamhetssystem, samt för projekt, se vidare nedan under punkt 4 *Genomförda granskningar under året*. Det bör också tas fram dokumentation

kring hur ofta informationsklassificeringar ska genomföras och hur resultatet av en klassificering ska tas om hand, för att tillse att erforderliga säkerhetslösningar för våra personuppgiftsbehandlingar implementeras. Slutligen bör bolaget ha en dokumenterad process för en regelbunden översyn av behörigheter i våra olika verksamhetssystem, hur och vem som kan bevilja behörigheter och hur behörigheter ska ändras eller tas bort vid uppsägning eller byte av tjänst.

DSO rekommenderar också att styrdokumentet Skyddade personuppgifter får en utpekad dokumentägare och att det under året uppdateras.

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?	16 av 60 (informationsklassningarna gäller inte personuppgiftsbehandlingarna utan de system i vilka behandlingarna 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 16 av 60 behandlingar. Klassningarna, som omfattar verksamhetssystemen Bostoc, Lime och Agda (och som innehåller merparten av personuppgifterna som bolaget behandlar), har genomförts under 2021 och är därmed aktuella. En handlingsplan för att åtgärda brister i organisatoriska och tekniska skyddsåtgärder finns framtagna i KLASSA. Dock har någon kontroll av huruvida lämpliga skyddsåtgärder faktiskt vidtagits med anledning av klassningen inte genomförts inom ramen för 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
X	**Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga**
	Inga brister av nämnvärd betydelse identifierade

Metodiken kring informationsklassning och SKR:s verktyg KLASSA bygger på att stadens förvaltningsmodell tillämpas och att det finns utsedda roller och utpekade ansvariga att lämna resultatet av informationsklassningen samt behovet av identifierade skyddsåtgärder till.

Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare. Det är en brist att bolaget ännu inte har utpekade informationsägare för exempelvis verksamhetssystemen Bostoc och Lime. Det är en förutsättning för att informationsklassningar genomförs regelbundet och att lämpliga skyddsåtgärder för personuppgifterna implementeras och upprätthålls.

3.3.5 DSO ger råd och rekommendationer till PUA

Det pågår ett arbete på bolaget att etablera en förvaltningsmodell och därigenom utse roller och utpekade ansvariga för genomförande

av informationsklassningar och att eventuella identifierade brister åtgärdas och risker minimeras.

Sedan ansvariga i organisationen pekats ut rekommenderar DSO att en rutin sätts upp där ansvariga årligen ser över behovet av klassning och/eller uppdatering av befintlig klassning och i samband med teritalrapport 2 rapporterar detta till informationssäkerhetssamordnare.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

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

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). IMY har publicerat en förtydligande förteckning över när personuppgiftsbehandlingar kräver en konsekvensbedömning. 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

Kontrollen har tagit avstamp i bolagets registerförteckning vilken ger en översiktsbild av vilka kategorier av personuppgifter som behandlas (exempelvis känsliga personuppgifter) samt vad som görs

med dessa uppgifter. Mot bakgrund av IMYs lista över behandlingar som kräver att konsekvensbedömning genomförs, kan åtminstone 2-3 av bolagets behandlingar antas leda till en hög risk för de registrerade ur ett integritetsperspektiv. Dessa har dock inte närmare analyserats för att konstatera huruvida en konsekvensbedömning behöver göras eller inte.

Inför implementeringen av ärendehanterings- och CRM systemet Lime gjordes det första steget av en konsekvensbedömning av den tänkta personuppgiftsbehandlingen i systemet. Denna initierades av DSO eftersom det handlade om implementering av ett nytt verksamhetssystem (ny teknik). Analysen resulterade i att en fullständig konsekvensbedömning inte behövde göras.

I övrigt har inga riskanalyser eller konsekvensbedömningar gjort av de behandlingar som kan antas leda till en hög risk.

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
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

Konsekvensbedömningen ser till att integritetsriskerna för personuppgifter som behandlas i projekt eller linjeverksamhet identifieras och minimeras. Risker kopplade till en viss behandling blir dokumenterade samt bedömda utifrån sannolikheten och konsekvensen om riskscenariot skulle inträffa. Baserat på bedömningen ska riskförebyggande åtgärder vidtas. Det är en brist att eventuellt behov av en konsekvensbedömning avseende behandling av känsliga personuppgifter inom förtursverksamheten samt behandling av sekretesskyddade personuppgifter inte har genomförts. Det är vidare en brist att behandlingen av personuppgifter i verksamhetssystemen inte har analyserats utifrån att det rör sig om en stor mängd personuppgifter om en stor mängd registrerade.

3.4.5 DSO ger råd och rekommendationer till PUA

DSOs rekommendation är att samtliga avdelningschefer får i uppdrag att i samband med att registerförteckningarna ses över vid rapporteringen av internkontrollen i tertialrapport 2 tillse att verksamheten också har kontrollerat behovet av konsekvensbedömningar. Vid behov ska verksamheten ha genomfört konsekvensbedömning senast vi utgången av 2022. Rapportering ska ske till DSO.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	21 begäran om tillgång 9 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 Integritetsskyddsmyndigheten (”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

21 begäran om registerutdrag och 9 begäran om radering har inkommit under 2021. 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. Möjligheter att radera uppgifter på begäran av den registrerade är begränsade med hänsyn till offentlighetsprincipen. Det finns standardiserade svar gällande detta när begäran inkommer. Dock saknas rutiner för radering när uppgifter ska raderas med anledning av felregistrering, se vidare nedan under punkt 3.5.5.

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.

Vad gäller rätten till radering är denna som nämnts ovan begränsad på grund av offentlighetsprincipen. Det har dock förekommit att registrering av personuppgifter skett helt felaktigt i bolagets verksamhetssystem. Dessa uppgifter ska inte sparas med hänvisning till offentlighetsprincipen utan gallras med hänvisning till det generella gallringsbeslutet, SSA 2016:01. Detta har skett en gång under året och det är en rekommendation att en rutin dokumenteras för hur radering kan ske i Bostoc, Lime samt Agresso när detta inträffar.

Slutligen bör nämnas att det saknas möjligheter att få ut automatiserade registerutdrag från verksamhetssystemet Bostoc, 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 är detta dock hanterbart. Skulle volymen av förfrågningar öka är det dock en rekommendation att se över en automatisering av hantering av registerutdrag för att kunna leva upp till Dataskyddsförordningens krav och begränsa arbetsinsatsen för varje enskild förfrågan.

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?	8
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	0
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	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

8 personuppgiftsincidenter har dokumenterats under året. Ingen av de dokumenterade incidenterna har bedömts vara så allvarliga att de rapporterats till IMY eller till de berörda personerna.

Av de totalt 8 rapporterade incidenterna rör 5 uppladdning av intyg och/eller kreditupplysning i fel kundärende. Totalt har felaktig hantering av intyg och/eller kreditupplysning i verksamhetssystemen rapporterats 15 ggr under året (varav 5 har bedömts vara en personuppgiftsincident enligt ovan). Det finns en dokumenterad rutin för hur detta ska hanteras på bolaget när det inträffar. Det pågår ett arbete med att automatisera hanteringen av kreditupplysningar, för att minska risken för att detta inträffar.

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

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. Detta gäller dock inte övergripande på hela bolaget, och det finns brister som kan leda till att personuppgiftsincidenter inte kan dokumenteras och rapporteras i tid.

3.6.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att processen för hantering av personuppgiftsincidenter, samt hur rapportering ska ske, tydligare gås igenom och informeras om till samtliga avdelningar i bolaget. Mot bakgrund av att bolaget behandlar en stor mängd personuppgifter i sina verksamhetssystem bör PUA tillse att samtliga avdelningar har förståelse för vad en personuppgiftsincident kan vara och att olika fel eller buggar i verksamhetssystemen sannolikt också innebär en personuppgiftsincident. Det bör tydliggöras vad syftet med att dokumentera och rapportera personuppgiftsincidenter är samt att bristande förmåga att rapportera personuppgiftsincidenter i tid kan leda till sanktioner från IMY. DSO bör genomföra utbildningsinsatser gällande detta under 2022.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Registerförteckningen
- Inbyggt dataskydd och dataskydd som standard
- Behandling av sekretesskyddade personuppgifter

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 - Registerförteckningen

Registerförteckningen ses över och uppdateras årligen och senast vid rapporteringen av interkontrollplanen till tertialrapport 2. Registerförteckningen har setts över och gåtts igenom avdelnings- och enhetsvis tillsammans med DSO. DSO har också gjort en allmän uppdatering med anledning av att ett nytt formulär för registerförteckningen togs fram centralt i staden, samt med anledning av att bolaget har genomfört informationsklassningar av verksamhetssystemen.

	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 ger en rättvisande bild av bolagets personuppgiftsbehandlingar och att den håller god kvalitet.

Granskning 2 – Inbyggt dataskydd och dataskydd som standard

Inbyggt dataskydd handlar om att ta hänsyn till dataskydd och integritetsskyddsregler redan när nya IT-lösningar designas, utvecklas, inköps eller anpassas eller vid utformning av nya rutiner, processer och liknande. Dataskydd som standard handlar om att de mest integritetsskyddande alternativen sätts som standard och att personuppgifter inte behandlas i onödan. I bolagets internkontrollplan för 2021, under granskningsområdet Dataskydd, finns en kontrollaktivitet som avser kontroll av att befintliga och nya it-system lever upp till krav på inbyggt dataskydd och dataskydd som standard. I samband med denna kontroll granskades bolagets dokumentation och rutiner kring detta, och avdelningschef för avdelningen för Digitala tjänster tillfrågades också om status.

	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

Det saknas dokumenterade rutiner eller styrdokument för hur verksamheten ska säkerställa inbyggt dataskydd och dataskydd som standard i exempelvis utveckling av nya system, systemförbättringar, upphandlingar eller i projekt. Detta är en brist som indikerar att inbyggt dataskydd och dataskydd som standard inte uppfylls i befintliga system och utvecklingsprojekt.

För det nyligen upphandlade ärendehanteringssystemet Lime har grundläggande krav på dataskydd ställts i upphandlingen, vilket

indikerar att det systemet bör ha tillfredsställande efterlevnad av principerna för inbyggt dataskydd och dataskydd som standard. Vad gäller befintliga IT-lösningar såsom verksamhetssystemet Bostoc arbetas det kontinuerligt med förbättrade säkerhets- och dataskyddslösningar. Det finns emellertid brister. Exempelvis samlas vid registreringstillfället fler personuppgifter in än vad som är nödvändigt för att registrera sig i bostadskön. Personuppgifter sparas också på flera olika ställen i systemen, utan direkt koppling till kundärendet, vilket leder till bristande översikt och kontroll på personuppgifter. I Bostoc finns behörighetsgrupper, exempelvis för sekretesshandläggare eller förtur, dock inga behörighetsnivåer för exempelvis vissa ärenden. Detta är en brist eftersom fler handläggare får åtkomst till personuppgifter än vad som behövs för att utföra sina arbetsuppgifter. Vidare är det en brist att loggning endast finns då personuppgifter ändras i systemen, dock inte för när handläggare/användare endast läser personuppgifter.

DSOs rekommendation är att upprätta ett styrdokument eller ett internt regelverk för inbyggt dataskydd och dataskydd som standard som ska tillämpas vid systemutveckling, upphandling av nya system och större projekt som omfattar personuppgiftsbehandling, för att säkerställa att de grundläggande principerna för dataskydd beaktas i nya och befintliga system och verksamhetsprocesser.

Granskning 3 – Behandling av sekretesskyddade personuppgifter

Bolaget behandlar i sina verksamhetssystem personuppgifter som efter beslut av Skatteverket är sekretesskyddade. Skyddade personuppgifter är Skatteverkets samlingsrubrik för de olika skyddsåtgärderna skyddad folkbokföring, sekretessmarkering och fingerade personuppgifter inom folkbokföringen. Rutiner för en enhetlig och säker hantering av skyddade personuppgifter är en förutsättning för att kunna upprätthålla skyddet. Under året har ett arbete med att uppdatera rutinerna för hantering av skyddade personuppgifter genomförts. Arbetet har resulterat i förbättrade rutiner kring hur bolaget kommunicerar med kunder med skyddade personuppgifter. Arbetet pågår alltjämt. Det utreds möjligheter att implementera en tjänst för att kunna skicka säkra meddelanden till dessa kunder, samt för att säkerställa en enhetlig och säker hantering generellt över bolaget.

Granskningen har omfattat kontroll av styrdokument och rutinbeskrivningar gällande hantering av skyddade personuppgifter samt intervjuer med företrädare för verksamheten i form av

verksamhetsutvecklare på Förmedlingsavdelningen, enhetschef för Förtursenheten samt enhetschef för Kundservice.

	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

Bolaget har en policy och rutin för skyddade personuppgifter som fastställdes av styrelsen 20161123 ”Skyddade personuppgifter – policy och handläggning”. Den består dels av en övergripande beskrivning av vad skyddade personuppgifter är och hur de ska hanteras, vilken följer den stadsövergripande policyn i staden, dels en mer verksamhetsspecifik del, med anvisningar särskilt för arbetet på bolaget. Generellt bedömer DSO att detta styrdokument håller god kvalitet och ger god ledning gällande hur hanteringen på bolaget ska ske. Det har dock uppmärksammats vissa brister i rutinerna, bland annat står att visningskallelser kan skickas via e-post till dessa kunder. E-post är inte en säker kommunikationskanal. Hanteringen kring detta har åtgärdats under året, men styrdokumentet behöver uppdateras därefter.

Genom intervjuerna har framkommit att styrdokumenten och rutinbeskrivningarna är ett stöd i det dagliga arbetet med skyddade personuppgifter, att de i huvudsak efterföljs av medarbetare som arbetar med skyddade personuppgifter och att den dokumentation som finns är tillräcklig.

Bostadssökandes möjligheter att identifiera sig med BankID eller motsvarande via telefon även vid kontakt med Förmedlingsavdelningen och Förtursavdelningen bedöms av verksamheten öka säkerheten i hanteringen av dessa kunder.

DSO bedömer att rutinerna kring hantering av skyddade personuppgifter finns på plats och efterlevs. Det arbete som utförts under året gällande förbättrade arbetssätt och rutiner har lett till en säkrare hantering och det är bra att arbetet prioriteras av verksamheten. Det är också positivt att nya tekniska funktioner, såsom krypterade meddelanden och legitimering via BankID, är under utredning och möjlig implementering under nästa år.

Det bör noteras att det finns brister i verksamhetsystemen Bostoc och Lime gällande markering och behörighetsbegränsning av uppgifter som har sekretess. Dessa tekniska brister har dock inte kontrollerats närmare inom ramen för denna granskning eftersom det i första hand avser funktioner i de it-system vari bolaget behandlar personuppgifterna. Dessa brister bör tas om hand inom ramen för handlingsplaner och förvaltningsplaner som rör dessa system.

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:

- Bristande uppfyllande av principen om lagringsminimering
- Intyg- och kreditupplysningshantering i verksamhetssystemen
- Bristande uppfyllande av principen om uppgiftsminimering

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

Bolagets nu gällande gallringsbeslut från 2013 föreskriver ett helhetsbevarande av informationen i verksamhetssystemet Bostoc. Den bakomliggande orsaken var att systemkopplingar i Bostoc krävde ett utökat bevarande i förhållande till föregående gallringsbeslut. Bevarandet av informationen bygger i huvudsak därför inte på verksamhetens behov av informationen, de registrerades integritet eller allmänhetens rätt till insyn, utan i första hand på tekniska svårigheter med att gallra. Eftersom det finns drygt 730 000 personer registrerade i bostadskön och dessa personers uppgifter sparas även sedan de avregistreras, behandlar bolaget stora mängder personuppgifter om många registrerade. Detta är i sig en risk. Offentlighetsprincipen och arkivlagen har företräde framför Dataskyddsförordningen. Bolagets gallringsbeslut föreskriver ett helhetsbevarande av informationen i verksamhetssystemet Bostoc. Risken utgör inte en brist i förhållande till efterlevnaden av Dataskyddsförordningen i sig, eftersom offentlighetsprincipen har företräde och bolaget förhåller sig till gällande lagstiftning och gallringsbeslut. Dock är det en risk att ha denna typ av gallringsbeslut eftersom det resulterar i att stora mängder personuppgifter sparas under en väldigt lång tid.

	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

Förslag till nytt gallringsbeslut för bolagets verksamhetsprocesser är under arbete. DSO rekommenderar att PUA tillser att förslaget till nytt gallringsbeslut antas och att de nya gallringsfristerna tillämpas.

Risk 2 – Intyg- och kreditupplysningshanteringen i verksamhetssystemen

Vid en förmedlingsprocess av en hyresrätt inhämtas intyg av bostadssökande till styrkande av att den sökande uppfyller hyresvärdens villkor. Intygen omfattar i regel anställningsintyg och lönespecifikationer, men kan även vara studieintyg, pensionsunderlag, olika utdrag från Försäkringskassan m.m. Kreditupplysning inhämtas också på den bostadssökande och

eventuell medboende. Så som systemstödet ser ut idag behöver kreditupplysningar och intyg manuellt laddas upp i den bostadssökandes ärende. Många sökandens ärenden hanteras samtidigt och tempot i förmedlingsprocessen är ofta högt. Detta gör att det händer att intyg och/eller kreditupplysningar sparas i fel kunds ärende. Eftersom dokumenten, sedan de sparats i kunds ärende, kan nås från kundens ”Mina Sidor” och de också i vissa fall skickas över till hyresvärden med hyresgästförslag, så blir personuppgifterna tillgängliga för obehöriga. Detta räknas som en personuppgiftsincident.

	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

Bolaget har arbetat med att dels att förbättra funktionerna i Bostoc, dels med rutinbeskrivningar för hanteringen av intyg. Implementeringen av det nya verksamhetssystemet Lime har också minskat risken för felhantering. Därtill har ett arbete pågått med leverantören av kreditupplysningstjänster för att förbättra integrationen mot bolagets verksamhetssystem. Trots detta kvarstår bristerna och DSO rekommenderar att arbetet med att minimera risken för en personuppgiftsincident vid uppladdning av intyg och/eller kreditupplysning fortsätter under 2022.

Risk 3 – Bristande uppfyllande av principen om uppgiftsminimering

En av de grundläggande principerna i Dataskyddsförordningen är uppgiftsminimering. Den innebär att fler personuppgifter än vad som är nödvändigt för att uppfylla ändamålet inte ska samlas in och behandlas.

Vid registrering i bostadskön via bolagets webbplats eller via blankett efterfrågas uppgifter som inte är nödvändiga för ändamålet att hantera bostadskön. Exempel på det är yrke, arbetsgivare och inkomst samt nuvarande boende, hyresvärd och hyra. DSO rekommenderar att registreringssidan och ansökningsblanketter ses

över och görs om så att personuppgifter som bara är nödvändiga samlas in vid registreringstillfället. Först när en bostadssökande är aktuell för förmedling av ett hyreskontrakt kan ytterligare personuppgifter hämtas in, såsom inkomstuppgifter och nuvarande boendesituation.

5.4 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:

- *Konsekvensbedömningar*
- *Uppgiftsminimering*

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 årsrapport. 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

Genom granskningen av det obligatoriska granskningsområdet ”konsekvensbedömning” framkom brister i och med att det sannolikt finns personuppgiftsbehandlingar som kan antas innebära en hög risk men som inte har konsekvensbedömts av verksamheten. DSOs rekommendation är att avdelnings- och enhetschefer får i uppdrag att i samband med översynen av registerförteckningen också bedöma sin verksamhets behov av en konsekvensbedömning. Resultatet bör redovisas senast vid utgången av 2022. DSO ska granska huruvida verksamheten genomfört nödvändiga konsekvensbedömningar. Resultatet av granskningen redovisas i årsrapporten för 2022.

Granskning 2

En risk som identifierats är att fler personuppgifter än vad som är nödvändigt för ändamålet samlas in vid registreringstillfället (se punkt 5.3 ovan). DSO ska under nästa år kontrollera hur registrering på bolagets webbplats och via blanketter sker i syfte att bedöma om principen om uppgiftsminimering uppfylls vid inhämtandet av personuppgifter. Resultatet redovisas i årsrapporten för 2022.