Stockholms stad

Bilaga 3

Ledningens genomgång år 2025

Bostadsförmedlingen i Stockholm AB

Beslutad xxxx-xx-xx

Ledningens genomgång

Dnr: BOST 2025/117

Kontaktperson: Pontus Ericson

1 Sammanfattning

För att nå stadens mål om en modern, hållbar och innovativ storstad ska det drivas ett systematiskt informationssäkerhetsarbete inom nämnder och styrelser. Informationssäkerhetsarbetet ska anpassas till de lokala behoven och ansvaret är därför decentraliserat i staden.

Enligt standarden ISO 27001 är ett LIS (Ledningssystem för informationssäkerhet) den del av det övergripande ledningssystemet som ska upprätta, införa, driva, övervaka, granska, underhålla och förbättra informationssäkerheten. Bolagets LIS omfattar alla de rutiner, processer, roller, ansvar och beslut som styr informationssäkerhetsarbetet i bolagets verksamhet, på lokal nivå.

Samtliga bolag ska i enlighet med stadens anvisningar för nämndernas arbete med verksamhetsplan 2026 ta fram ”Ledningens genomgång” med en planering för informationssäkerhetsarbetet under de kommande tre åren. Denna biläggs verksamhetsplanen och redovisas i verksamhetsplanen under mål 3.5. Genomgången innefattar bedömningar av möjligheter till förbättring och behovet av förändringar i LIS, inklusive mål för informationssäkerheten.

Alla nämnder och bolagsstyrelser ska prioritera att ta fram en plan för att inventera och klassa information som används i verksamheten alternativt se över och uppdatera genomförda klassningar. Stadens prioritering ligger i linje med den plan för den kommande perioden som bolaget upprättat och som redovisas i detta dokument. Utöver kontinuerlig uppdatering av registerförteckningar och återkommande informationsklassningar kommer bolagets informationssäkerhetsarbete under den kommande perioden vara inriktat mot förbättringar i bolagets verksamhetssystem, med särskilt fokus på behörighetsstruktur samt loggning. Vidare kommer bolagets informationssäkerhetssamordnare (ISAM) under den kommande perioden fortsätta att utbilda ledning och medarbetare i informationssäkerhetsfrågor.

Innehållsförteckning

1 Sammanfattning 3

1.1 Faktorer som påverkar verksamhetens LIS 5

1.1.1 Ledningssystem för informationssystem, LIS. 5

1.1.2 Om bostadsförmedlingens verksamhet med avseende på dataskydd och informationssäkerhet. 5

1.1.3 Resultatet från egen uppföljning (VoR och IKP) 6

1.1.4 Resultatet från revisioner 6

1.1.5 Risker som identifierats i GDPR-årsrapport 7

1.1.6 Information om avvikelser (incidenter och andra händelser) 7

1.2 Förbättringar som föreslås för verksamhetens LIS 7

1.2.1 Uppdatera Lokal anvisning 7

1.2.2 Följa upp utbildningsinsatser för chefer och medarbetare 8

1.2.3 Genomföra inventering, konsekvensbedömningar och klassning 8

1.2.4 Incidenthantering 9

1.1 Faktorer som påverkar verksamhetens LIS

Ledningens genomgång ska baseras på ett strukturerat underlag som omfattar samtliga faktorer som kan påverka verksamhetens LIS. Dessa faktorer redogörs för nedan.

1.1.1 Ledningssystem för informationssystem, LIS

Stockholms stads arbete med informationssäkerhet utgår från en så kallad ISO standard, ISO 27001. Det är en global standard för informationssäkerhet som hjälper organisationer att skydda sin känsliga information från hot och risker. Standarden ger ett ramverk för hur man implementerar ett ledningssystem för informationssäkerhet, LIS, som skyddar informationstillgångarna och ger en IT-process som är lättare att hantera, mäta och förbättra.

Stockholms stads informationssäkerhetsarbete regleras i en tillämpningsanvisning som är en bilaga till stadens kvalitetsprogram. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören.

Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete. Bolagets VD har fastställt en så kallad lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom Bostadsförmedlingen.

1.1.2 Om bostadsförmedlingens verksamhet med avseende på dataskydd och informationssäkerhet.

Bostadsförmedlingen har cirka 890 000 registrerade kunder (bostadssökande) och förmedlar ca 20 000 lägenheter om året.

För att kunna fullgöra sitt uppdrag inhämtar bolaget en stor mängd information om kunden vid förmedling av lägenhet. Några exempel på sådan information är namn, personnummer, adress, e-post, telefonnummer, uppgift om köavgift, tid i bostadskön, barn i hushållet, medboende, sysselsättning, arbetsgivarens namn, årsinkomst samt gjorda intresseanmälningar och visningskallelser. Bolaget hanterar i sin förmedlingsverksamhet även lönespecifikationer, kreditupplysningar, uppgifter om bidrag, sjukintyg, intyg från försäkringskassan och andra dokument som kan styrka att krav på kundens betalningsförmåga uppnås.

En stor och viktig del av bolagets informationssäkerhetsarbete handlar om att säkerställa att alla de personuppgifter bolaget behandlar och som redovisas ovan hanteras på ett ändamålsenligt och säkert sätt.

Ett annat prioriterat område inom bolagets informationssäkerhetsarbete handlar om bolagets kärnverksamhet, själva förmedlingen av hyreslägenheter. En lägenhet i Stockholm är mycket eftertraktad, vilket också innebär en risk för att människor söker vägar för att tillskansa sig en lägenhet på ett lagvidrigt sätt eller på oriktiga grunder. Det är av yttersta vikt att bolagets förmedlingsprocess är och uppfattas som rättvis, transparent och rättssäker. Att tillse att information i bolagets system om till exempel kötid inte kan manipuleras är en kärnpunkt i bolagets informationssäkerhetsarbete. Här ställs stora krav på såväl systemstödet i sig och på bolagets interna processer och kontrollmekanismer.

Hur viktiga och prioriterade informationssäkerhetsfrågorna är inom bolaget, speglas bl a av att vi samorganiserat expertkompetens på informationssäkerhet med expertkompetens på IT-säkerhet i kvalitetshöjande syfte.

1.1.3 Resultatet från egen uppföljning (VoR och IKP)

Bolaget säkerställer i enlighet med kommunfullmäktiges direktiv att det finns ett effektivt och ändamålsenligt informationssäkerhetsarbete. Arbetet har under perioden fortlöpt enligt plan.

I bolagets internkontrollplan ska årlig kontroll göras av att alla registerförteckningar är uppdaterade och ger en rättvisande bild av bolagets personuppgiftsbehandlingar.

Internkontrollplanen (IKP) innehåller också årlig kontroll av behörigheter för respektive system samt av behörighetsregistren.

Efter genomförd väsentlighets- och riskanalys (VoR) har ett behov av följande åtgärder identifierats:

- Resultaten av regelbundna klassningar ska omhäntertas inom respektive ansvarsområde.

- Skapa organisatoriska förutsättningar för att bedriva ett systematiskt informationssäkerhetsarbete. Utöka de personalresurser som ansvarar för att driva de strategiska informationssäkerhetsfrågorna på bolaget och löpande vidareutbilda chefer och medarbetare på informationssäkerhetsområdet.

- Ta fram rutin för att säkerställa att informationssäkerhetsaspekter finns med, beaktas och vid behov kravställs vid upphandling på bolaget.

- Underhålla och sprida kunskapen om befintlig lokal rutin för behörighetshantering samt att fortsatt minst årligen genomlysa samtliga behörigheter i bolaget samtliga systemstöd.

1.1.4 Resultatet från revisioner

Särskilda granskningar av bolagets dataskyddsarbete har genomförts under 2024. De förbättringsförslag som identifierades har åtgärdats under 2025. Åtgärderna har rapporterats till styrelsen.

1.1.5 Risker som identifierats i GDPR-årsrapport

Risker som identifierades i 2024 års GDPR-årsrapport har till största del åtgärdats, särskilt genom framtagande av fler erforderliga styrdokument samt gjorts tillgängliga och kända för medarbetarna genom publicering av dessa på bolagets intranät.

1.1.6 Information om avvikelser (incidenter och andra händelser)

Det finns inga incidenter under föregående år som bedöms vara av den graden att det behöver omnämnas här. Dock har vissa personuppgiftsincidenter inträffat under föregående vilka är beskrivna i dataskyddsombudets årsrapport.

1.2 Förbättringar som föreslås för verksamhetens LIS

1.2.1 Uppdatera Lokal anvisning

Den lokala anvisningen togs fram och fastställdes av VD under 2022. Denna ska enligt bolagets rutin ses över, och vid behov uppdateras, i samband med den årliga översynen av samtliga styrdokument vid årets sista styrelsemöte under de kommande tre åren. Anvisningen har under 2025 setts över och till viss del uppdaterats

1.2.2 Följa upp utbildningsinsatser för chefer och medarbetare

Under 2024 genomfördes en större utbildningsinsats för både chefer och medarbetare, och av den anledningen har utbildningsinsatsen under 2025 inte behövt vara lika omfattande. Arbetet kommer att fortsätta även under 2026 och då med mer information och utbildning. Information och utbildning inom informationssäkerhet och dataskydd är även återkommande punkt på bolagets s.k. ”chefsforum” där samtliga chefer på bolaget deltar.

Stadens centrala funktion för informationssäkerhet lanserade under 2024 nya e-utbildningar till chefer och medarbetare. Dessa är obligatoriska och det åligger chefer med medarbetaransvar att tillse och följa upp att utbildningarna genomförs

1.2.3 Genomföra inventering, konsekvensbedömningar och klassning

I oktober 2025 beslutades det om en rutin för registerförteckningen, där det fastslogs att granskning av registret ska göras årligen, senast i oktober månad. Det är utsedd behandlingsansvarig som ansvarar för att granskningen görs. DSO granskar registret årligen efter att intern granskning är genomförd.

I uppföljningen av internkontrollplanen står det; *att kontroller sker löpande i arbetet med att upprätthålla och uppdatera bolagets registerförteckningar samt genom att rutiner gällande dataskydd följs i verksamheten. Kontroll av att registerförteckningarna ger en rättvisande bild av verksamhetens personuppgiftsbehandlingar och är uppdaterad (art 30 GDPR). Kontroll av att de lokala anvisningarna för informationssäkerhet implementerats planenligt.*

De interna granskningar som genomförts av behandlingsansvarig under året, avseende registerförteckningar, visade inte på några avvikelser.

Informationsklassning har skett av informationsmängderna bolagets samtliga lokala verksamhetssystem samt ekonomisystemet.
Enligt bolagets lokala anvisning för informationssäkerhet ska informationsklassningar uppdateras eller genomföras årligen.

Särskilt fokus ligger här på verksamhetsprocesser som innehåller stora volymer av integritetskänsliga personuppgifter. Huvudsakligen rör detta uppgifter i verksamhetssystemet Bostoc som har informationsklassats vid ett flertal tillfällen.
Under de tre kommande åren kommer klassingsarbetet fortsätta enligt upparbetad rutin och planläggning.

Planerade åtgärder med anledning av genomförda informationsklassningar

De årliga informationsklassningarna resulterar i handlingsplaner där nödvändiga åtgärder som identifierats förtecknas, både vad gäller förändrade arbetssätt/ rutiner, dokumentation och systemutveckling.

För närvarande pågår ett större utvecklingsarbete med Bostoc+ projektet som ger förutsättningar till en högre nivå på informationssäkerhet, bland annat genom fler behörighetsnivåer.

Vidare pågår även projektet Bostadsportalen (tidigare benämnt Säker fastighetsportal) samt projektet BEMS som också bidrar till ökad informationssäkerhetsnivå genom att handhavande automatiseras och således minskar risker för att handläggare hanterar personuppgifter felaktigt.

1.2.4 Incidenthantering

Bolaget har en gemensam rutin för Personuppgiftsincidenter och informationssäkerhetsincidenter. Rapportering och hantering av incidenter ska ske enligt gällande rutin.

Under 2026 kommer granskning ske gällande hur väl incidentrutinen efterlevs i organisationen.