



---

**Tjänsteutlåtande**

Utfärdat 2026-04-13

Ärendenummer FGL-2025-00314

Handläggare

Petra Willquist Rönnäng

Telefon: 031-368 5514

E-post: [petra.willquist.ronnang@gotalejon.goteborg.se](mailto:petra.willquist.ronnang@gotalejon.goteborg.se)

## Lägesrapport implementering av Dora-förordningen - April

### Förslag till beslut

I styrelsen för Försäkrings AB Göta Lejon:

Styrelsen antecknar information om implementering av Dora-förordningen.

### Sammanfattning

Styrelsen har gett bolaget i uppdrag att lämna en lägesrapport kring tidplan och införande av Dora-förordningen. Bolaget har en planering och prognos för första och andra kvartalet 2026.

### Bedömning ur ekonomisk dimension

Som försäkringsbolag under Finansinspektionens tillsyn omfattas Göta Lejon av Dora-förordningen, vilken gäller sedan januari 2025.

### Bedömning ur ekologisk dimension

Bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

### Bedömning ur social dimension

Bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

### Bilagor som ingår i beslutsunderlaget

1. Uppföljning implementering Dora 2026-04-13 (Sekretess OSL 18:13)
2. Intraservices statusrapport av handlingsplan Dora kvartal 1

## Beskrivning av ärendet

EU-förordningen för digital operativ motståndskraft (Dora-förordningen) började gälla i januari 2025. Den innebär nya krav på i stort sett alla företag inom den finansiella sektorn när det gäller IKT-risker.

Dora-förordningen innebär bland annat att högre krav på företagen att:

- hantera risker inom informations- och kommunikationsteknologi (IKT)
- rapportera IKT-relaterade incidenter
- testa den digitala operativa motståndskraften
- hantera IKT-relaterade tredjepartsrisker.

Ovanstående punkter kallas även för Doras pelare. Dora-förordningen kompletteras av tekniska standarder som närmare specificerar de krav som finns i Dora-förordningen.

Styrelsen har efterfrågat en presentation av arbetet och tidplanen för implementering av Dora-förordningen. Göta Lejon redovisar nuläge och prognos för efterlevnad baserat på de fyra pelare som bolagets omfattas av. Bilagt ärendet är även Intraservices uppföljning av sin handlingsplan. Denna uppföljning redovisar avvikelser mot initial tidplan på två områden.

### **Pelare I: IKT-riskhantering**

Pelaren handlar bland annat om att företag ska ha en dokumenterad process för hur de hanterar IKT-risker och att det krävs kontinuerlig uppföljning av risknivåer. Pelaren anger även att styrelse och ledning måste vara involverade och ansvariga.

### **Pelare II: Incidenthantering**

Här ställs krav på rutiner för att upptäcka, analysera och rapportera IT-incidenter. Pelaren anger även rapporteringsskyldighet inom satta tidsramar till tillsynsmyndigheter vid allvarliga incidenter. Vidare ska kommunikation ske med kunder när incidenter påverkar deras tjänster.

### **Pelare III: Testning av digital operativ motståndskraft**

För att visa att verksamheten och systemen verkligen klarar störningar kräver DORA regelbunden heltäckande testning. Det kan handla om penetrationstester för att upptäcka sårbarheter men även krisövningar där större avbrott simuleras. Kritiska system ska kontinuitetstestas.

### **Pelare IV: Hantering av IKT-tredjepartsrisker**

Pelaren handlar om de krav som behöver ställas i avtal med leverantörer. Pelaren handlar även om riskbedömningar som ska göras innan nya leverantörer tas in. Leverantörers säkerhetsnivå ska löpande följas upp.

## **Bolagets bedömning**

Det är bolagets bedömning att informationen visar på bolagets handlingsplan för implementeringen av Dora-förordningen.

Petra Willquist Rönnäng

Anders Jonasson

Bolagscontroller

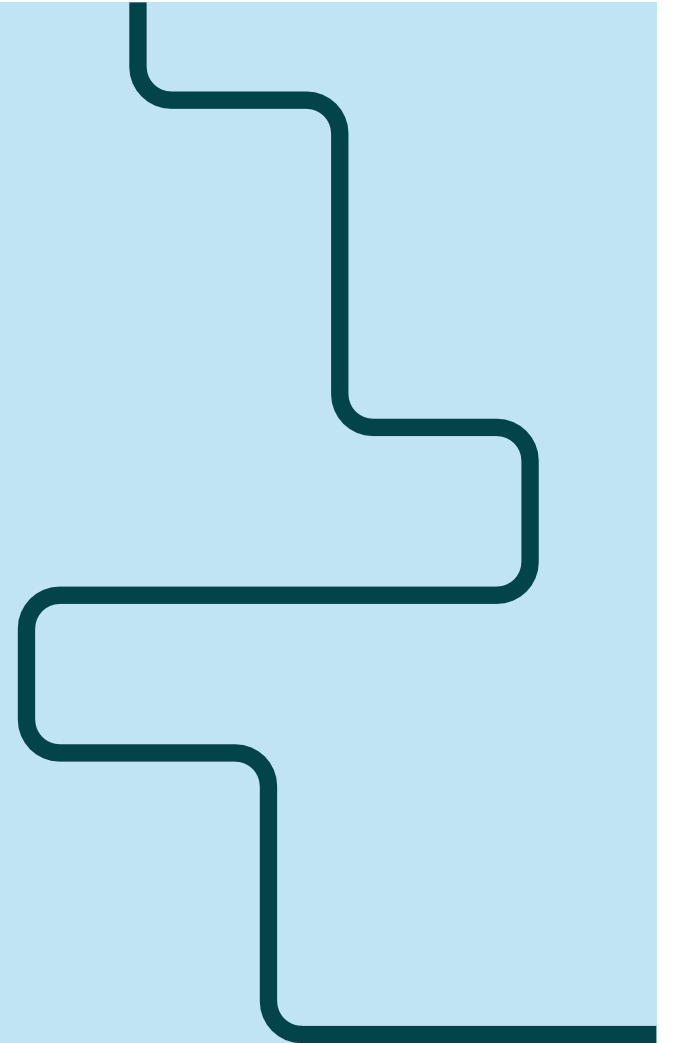
VD

# Säkerhets- och incidenthantering

## Uppföljning av beslutad handlingsplan

**Intraservice och Göta Lejon AB**

Uppföljningsrapport kvartal 1, 2026



# Lägesrapport över beslutade åtgärder



# Beslutad handlingsplan

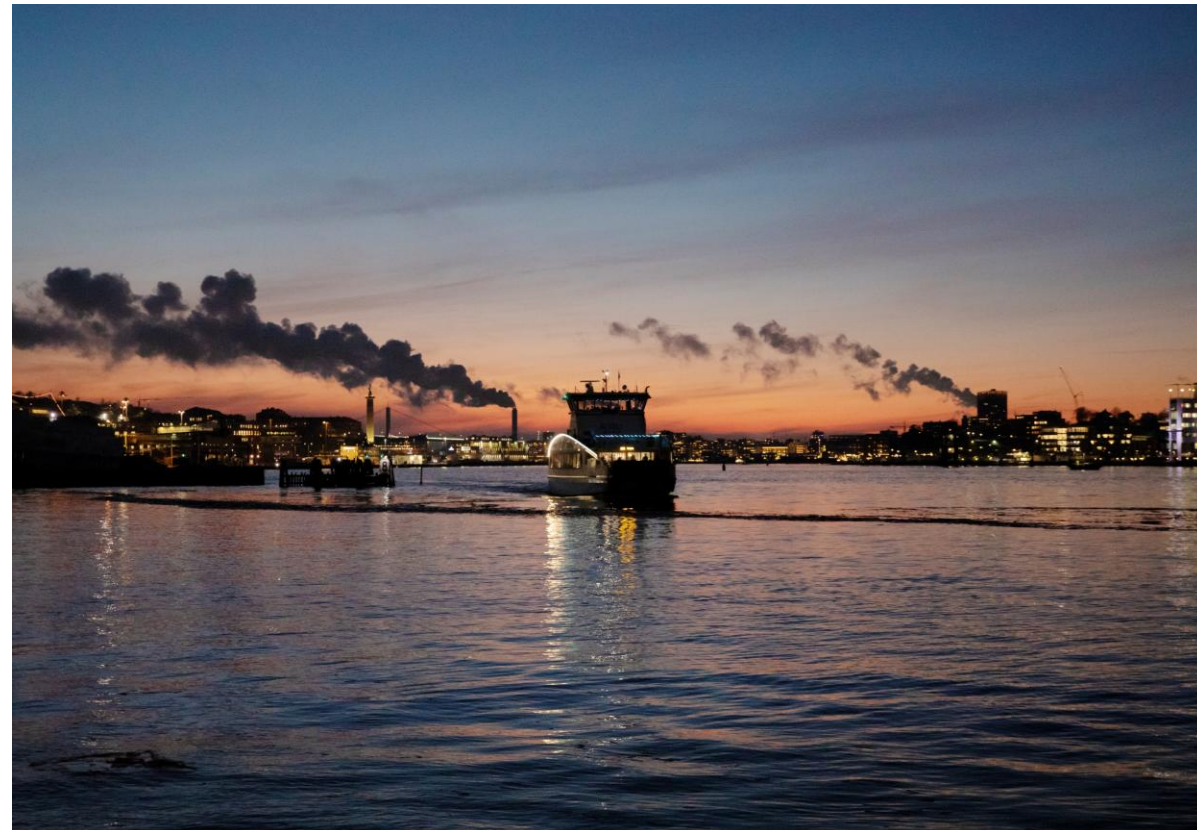
Nr	Åtgärd	Status
1a)	Incidenthantering på kort sikt	Avvikelse enligt initial tidplan
1b)	Incidenthantering på lång sikt	Pågår enligt plan
2	Säkerställa administrativa åtgärder	Pågår enligt plan
3	Unit 4 - Införa MFA	Pågår enligt plan
4a)	Unit 4 - Verifiera status på larmsättning och införda säkerhetsmekanismer	Pågår enligt plan
4b)	Verifiera status på larmsättning och införda säkerhetsmekanismer - Insman	Avvikelse enligt initial tidplan
5	Beställning av MFA - Insman	Avslutad/Stängd
6	Beställning av redundans – Insman	Avslutad/Stängd
7	Undersöka möjligheter för krypterad trafik	Pågår enligt plan
8	Delta i arbete med framtagning av use-cases för säkerhetsövervakning	Pågår enligt plan

# 1. Incidenthantering



## Avvikelse enligt initial tidplan

- » Vi har idag hantering av våra infrastrukturdelar bl.a. servrar och databaser och där känner vi oss trygga att vi uppfyller fastställda krav.
- » Det vi saknar idag är fullvärdig hantering kopplat till applikationsdelen Insman.
- » Arbete pågår inom projektet Införa systemstöd för cybersäkerhetslagen med usecases och acceptanstest kopplat till incidenthanteringen.
- » Fortsatt arbete och dialog krävs för att tydliggöra hanteringen av applikationsdelen.



Åtgärden har koppling till andra punkter i handlingsplanen. Arbetet hålls ihop inom programmet Införa cybersäkerhetslagen på Intraservice med utsedda projektledare för att säkerställa framdrift.

## 2. Säkerställa administrativa åtgärder

### Pågår enligt plan

- » Stadens nya riktlinje för informations- och cybersäkerhet är publicerad och gäller för stadens samtliga nämnder och styrelser.
- » Arbetet med att säkerställa administrativa åtgärder pågår enligt plan med målbild att säkerställa följsamhet mot ISO 27001.
- » Projektet Etablera systematiskt informationssäkerhetsarbete (ESI) pågår med framtagning av anvisningar och andra styrande dokument.
- » Flertalet anvisningar har tagits fram utifrån lokal tidplan för projektet.



Staden har sedan början av året en ny riktlinje för informations- och cybersäkerhet. Syftet med Göteborgs Stads riktlinje för informations- och cybersäkerhet är att skapa förutsättningar för ett systematiskt, riskbaserat och långsiktigt arbete.

# 3. Multifaktorautentisering Unit 4



## Pågår enligt plan

- » Åtgärden syftar till att säkerställa multifaktorautentisering för ekonomisystemet Unit 4 som gör att vi når rätt LOA-nivå (tillitsnivåer för e-legitimering).
- » Upphandling av ekonomisystem i staden pågår med införandeperiod fram till 2028. Fokus ligger på att säkerställa MFA kopplat till ekonomihanteringen.
- » Upphandlingsförfarandet av ekonomisystem avbröts vid årsskiftet på grund av bristande konkurrens. Nytt upphandlingsförfarande sker under 2026. Bedömningen är att detta inte kommer påverka beslutad tidplan i handlingsplanen.



Upphandling och införande av nytt ekonomisystem i staden pågår fram till 2028. Utifrån projektets tidplan och framdrift bevakar vi frågan gällande förutsättningar för multifaktorautentisering kopplat till ekonomihanteringen.

# 4. Larmsättning och säkerhetsmekanismer

## ● Avvikelse enligt initial tidplan

- » Vi har idag larmsättning på våra infrastrukturdelar bl.a. servrar och databaser och där känner vi oss trygga att vi uppfyller fastställda krav och förväntningar.
- » Det vi saknar idag är larmsättning på applikationsdelen Insman.
- » Gemensamt möte mellan Intraservice och Göta Lejon behövs för att tydliggöra hanteringen av applikationsdelen. Intraservice sammankallar till gemensamt möte.

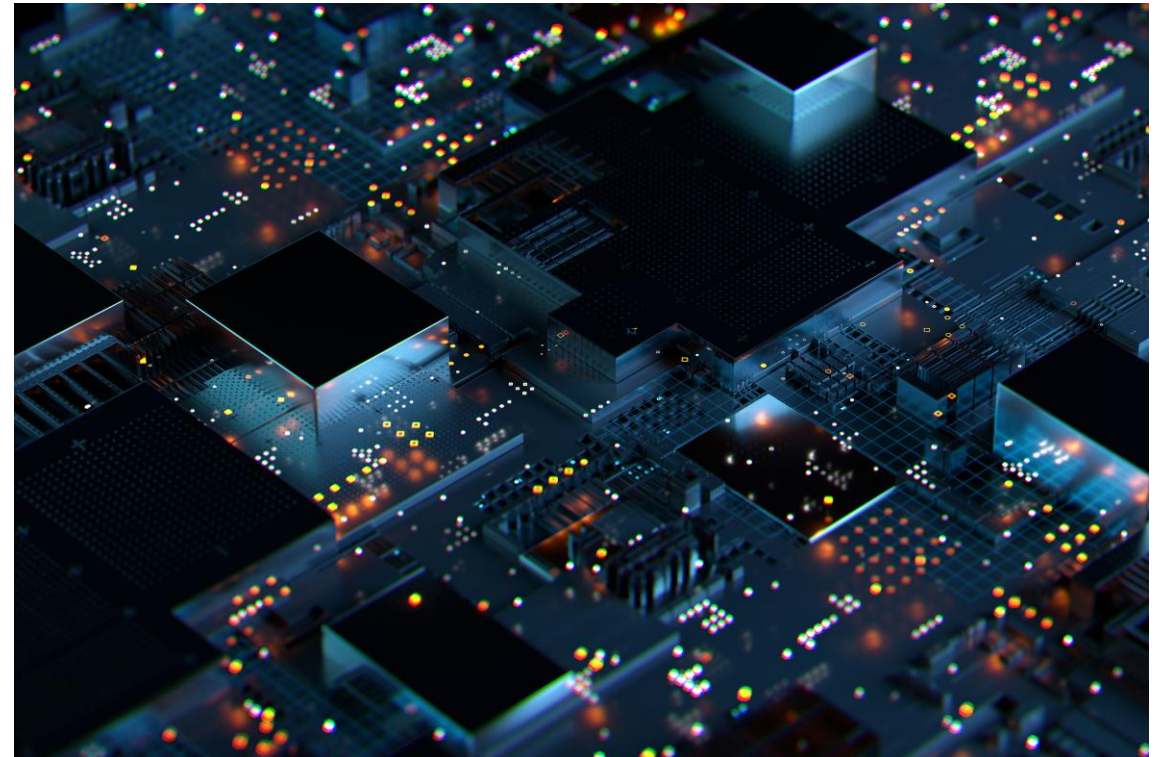


Åtgärden har koppling till andra punkter i handlingsplanen. Arbetet hålls ihop inom programmet Införa cybersäkerhetslagen på Intraservice med utsedda projektledare för att säkerställa framdrift.

# 5. Multifaktorautentisering Insman

## Klar/Avslutad

- » Beställning av autentisering med hjälp av sms-stöd är genomförd och implementerad
- » Nödvändig åtgärd är genomförd och aktiviteten är avslutad.



# 6. Redundans Insman

## Klar/Avslutad

- » Dialog mellan Intraservice och Göta Lejon har skett och lösning visad.
- » Nödvändig åtgärd är genomförd och aktiviteten är avslutad.



# 7. Krypterad trafik

## Klar/Avslutad

- » Kryptering av trafik finns idag för applikationsdelen.
- » Dialog har skett mellan Intraservice och Göta Lejon AB med bedömning att vi uppfyller kraven.
- » Nödvändig åtgärd är genomförd och aktiviteten är avslutad.



# 8. Usercases för säkerhetsövervakning

## Pågår enligt plan

- » Arbetet med att införa informationssäkerhetsdatabas (ISDB) pågår inom ramen för projektet Etablera systematiskt informationssäkerhetsarbete (ESI).
- » Initial dialog mellan Intraservice och Göta Lejon har skett för att se över behov att ingå i pilotinförande med PoC av ISDB.
- » Arbete genomfört tillsammans med Göta Lejon för genomgång av use-case och acceptanskriterier för PoC. Resultatet återkopplas till Göta Lejon.
- » Fortsatt dialog och samarbete mellan Intraservice och Göta Lejon sker under kvartal 2 enligt tidplan



Åtgärden har koppling till andra punkter i handlingsplanen. Arbetet hålls ihop inom programmet Införa cybersäkerhetslagen på Intraservice med utsedda projektledare för att säkerställa framdrift.



Göteborgs  
Stad