



Till  
Styrelsen i S:t Erik Försäkrings AB

## **Rapport för perioden 1 januari - 26 februari 2025 avseende regelefterlevnad**

### **1 Inledning**

Genom denna rapport redovisar funktionen för regelefterlevnad resultatet av senast genomförd kontroll av S:t Erik Försäkrings AB:s, nedan Bolaget, regelefterlevnad samt redogör för de övriga åtgärder som funktionen har vidtagit under perioden.

### **2 Händelser av relevans under perioden**

#### **2.1 Regelbevakning och relevanta sanktionsbeslut**

Under perioden har följande nyhetsbrev tillställts Bolaget. Dessa återfinns i sin helhet i [bilaga 1](#).

- Nyhetsbrev ang. Dora-förordningen.
- Nyhetsbrev ang. tjänster som bör anses vara IKT-tjänster enligt Dora.
- Nyhetsbrev ang. hållbarhetsrisker i skadeförsäkringsföretagens Orsa-rapporter.

#### **2.2 Kontroll av Bolagets regelefterlevnad**

Kontroll av Bolagets regelefterlevnad har ägt rum genom ett möte med representanter från Bolaget samt genom granskning av handlingar.

Kontrollen utgår från den årsplan som funktionen för regelefterlevnad har upprättat inför verksamhetsåret och redogörs för närmare nedan.

<i>Område</i>	<i>Kontroll</i>	<i>Compliancerisk (Grön/Gul/Röd)</i>
GDPR	Kontroll avseende dels hantering av personuppgifter i verksamheten, dels interna rutiner avseende uppföljning och kontroll.	Kontrollen har inte föranlett några synpunkter.
Rapportering	Kontroll avseende rapportering till Finansinspektionen.	Kontrollen har inte föranlett några synpunkter.
Övrig regelefterlevnad	Kontroll avseende Bolagets riktlinjer för riskhantering.	Kontrollen har inte föranlett några synpunkter.
Övrig regelefterlevnad	Kontroll avseende Bolagets rutiner och regler för återförsäkringsrisker.	Kontrollen har inte föranlett några synpunkter.

### Metod

Första kvartalets kontroll har till övervägande del bestått i att kontrollera Bolagets hantering av personuppgifter samt interna rutiner för denna hantering. Därtill har dataskyddsombudets årsrapport avseende internkontroll granskats utifrån reglerna i Dataskyddsförordningen.

Därtill har mer stickprovsbaserade kontroller utförts avseende rapportering, riktlinjer för riskhantering och återförsäkringsrisker. Gällande rapportering har funktionen för regelefterlevnad stämt av med Bolaget att relevant rapportering till Finansinspektionen har utförts. Gällande granskning av rutiner och riktlinjer har dessa dels diskuterats vid kontrollmöte med Bolaget, dels granskats av funktionen för regelefterlevnad mot bakgrund av relevanta regelverk.

### Relevanta regler och riktlinjer

Periodens kontroller baseras på följande regelverk och styrdokument i Bolagets verksamhet:

- Försäkringsrörelselag (2010:2043)
- FFFS 2015:8 om Försäkringsrörelse

- Dataskyddsförordningen (GDPR)
- DORA-förordningen
- Riktlinjer för riskhantering
- Rutiner för hantering av återförsäkringsrisker

### **GDPR - kontroll**

Granskning av Bolagets interna rutiner och riktlinjer i syfte att säkerställa att Bolaget uppfyller kraven på personuppgiftshantering i enlighet med dataskyddsförordningen.

Funktionen för regelefterlevnad har begärt in och granskat dels Bolagets interna riktlinjer för personuppgiftshantering, dels information som tillhandahålls publikt på hemsidan. Bolaget har redogjort för interna rutiner och riktlinjer för hantering av personuppgifter och därvid informerat funktionen för regelefterlevnad om att några större förändringar inte har varit påkallade sedan funktionens senaste kontroll och att det inte inträffat några personuppgiftsincidenter. Därtill har funktionen för regelefterlevnad granskat dataskyddsombudets årsrapport avseende år 2024.

Bolaget har vidare informerat funktionen för regelefterlevnad om att man har sett över olika alternativ för att byta ut Bolagets dataskyddsombud. Bolaget har överenskommit med Stockholm Stads serviceförvaltning att serviceförvaltningen ska biträda med denna tjänst fr.o.m. år 2025.

Funktionen för regelefterlevnad har inte haft några synpunkter med anledning av kontrollen.

### **Rapportering - Kontroll**

Granskning av Bolagets interna rutiner och riktlinjer för rapportering till Finansinspektionen. Kontrollen har syftat till att säkerställa att Bolaget vidtar rimliga åtgärder för att säkerställa ändamålsenlig rapportering till Finansinspektionen samt att det finns dualitet i Bolaget och rutiner för att rapportera till Finansinspektionen inom utsatt tid.

Vid mötet har Bolaget redogjort för Bolagets rutiner för att säkerställa ändamålsenlig rapportering i enlighet med ovan.

Funktionen för regelefterlevnad har inte haft några synpunkter med anledning av kontrollen.

### Övrig regelefterlevnad - Kontroll

- a) Uppföljning av Bolagets riktlinjer för riskhantering. Kontrollen har syftat till att säkerställa att riktlinjerna är ändamålsenliga och har det innehåll som krävs enligt bl.a. försäkringsrörelselagen (2010:2043) och Finansinspektionens föreskrifter och allmänna råd (FFFS 2015:8) om försäkringsrörelse.

Funktionen för regelefterlevnad har inte haft några synpunkter med anledning av kontrollen.

- b) Uppföljning och kontroll av Bolagets riktlinjer samt rutiner för återförsäkring. Kontrollen har syftat till att säkerställa att Bolagets regler och rutiner avseende återförsäkring är upprättade enligt gällande regelverk.

Funktionen för regelefterlevnad har granskat relevanta riktlinjer. Därtill har Bolaget och funktionen diskuterat återförsäkringsprogrammet samt justeringar som skett däri under år 2024.

Funktionen för regelefterlevnad har inte haft några synpunkter med anledning av kontrollen.

### **2.3 Råd och stöd**

Funktionen för regelefterlevnad har under perioden funnits tillgänglig för att svara på frågor och lämna råd och stöd till Bolagets anställda.

### **3 Funktionen för regelefterlevnads bedömning**

Funktionen för regelefterlevnad har vid fullgörandet av sitt uppdrag inte funnit något som innebär att Bolaget sammantaget inte lever upp till de krav som uppställs i de lagar, förordningar, föreskrifter och allmänna råd som gäller för Bolagets tillståndspliktiga verksamhet.

Stockholm den 26 februari 2025



Johan Grenefalk

## Nyhetsbrev

Ang. Dora-förordningen

---

17 januari 2025

### 1 Digital operativ motståndskraft inom finanssektorn

Idag ska EU:s förordning om digital operativ motståndskraft (Dora) börja tillämpas. Detta ställer krav på finansiella entiteter att hantera risker kopplade till informations- och kommunikationsteknik vilket innefattar att ställa krav på avtalsparter som levererar IKT-tjänster och att anpassa sina interna riktlinjer och rutiner.

Bland annat ska ett informationsregister upprättas och sändas in till Finansinspektionen i april 2025. Registret ska innehålla uppgifter om tredjepartsleverantörer av IKT-tjänster och deras underleverantörer. Det är därför viktigt att företagen har koll på vad som utgör en IKT-tjänst och vilka leverantörer som måste upptas i registret. Ett uppdaterat register ska därefter årligen skickas till Finansinspektionen och företagen bör därför ha rutiner för att kontinuerligt uppdatera registret när nya avtal som rör IKT-tjänster träffas.

Vidare ska finansiella entiteter uppmärksamma och rapportera allvarliga IKT-relaterade incidenter till Finansinspektionen. Eftersom tidsfristerna för inrapportering är relativt snäva måste företagen ha förmågan att snabbt upptäcka och identifiera när en allvarlig IKT-relaterad incident har ägt rum. För att klassificera incidenter ska företagen använda sig av olika tröskelvärden som i vissa fall kan vara svåra att överblicka. Det kan till exempel avse vilken geografisk spridning en incident har haft eller hur företagets anseende har påverkats.

När en allvarlig IKT-relaterad incident har inträffat ska initialt en första rapport tillställas Finansinspektionen, följt av delrapport och slutrapport.

### 2 Wesslau Söderqvist Advokatbyrås rekommendationer

Implementeringen av Dora kräver ett helhetsgrepp kring hur företagen arbetar med digital säkerhet och motståndskraft mot förluster och avbrott. Det är därför viktigt att företagen har klart för sig vilka åtgärder som behöver vidtas, samt i vilken utsträckning ytterligare data måste hämtas in för att fullgöra lagkraven. Vi på Wesslau Söderqvist Advokatbyrå har följt lagstiftningsarbetet från start och har bistått både finansiella entiteter och tredjepartsleverantörer av IKT-tjänster i implementeringsarbetet. Vi bevakar även löpande det pågående lagstiftningsarbetet beträffande frågor som ännu inte har klarlagts.



Om ni har frågor med anledning av Dora eller önskar vår hjälp i det fortsatta arbetet är ni varmt välkomna att höra av er till Wesslau Söderqvist Advokatbyrå.

## Nyhetsbrev

Ang. Tjänster som bör anses vara IKT-tjänster enligt Dora

---

28 januari 2025

### 1 Bakgrund

Europeiska kommissionen, nedan Kommissionen, har besvarat en fråga om vilka tjänster som bör anses vara IKT-tjänster enligt EU:s förordning om digital motståndskraft inom finanssektorn, nedan DORA.

Eftersom IKT-tjänster är ett nyckelbegrepp i DORA är det av stor vikt att alla aktörer som omfattas av regleringen har förståelse för begreppets definition för att säkerställa en korrekt efterlevnad av lagstiftningen. Svardsdokumentet som publicerats av EIOPA är avsett som ett stöd för att tolka begreppet "IKT-tjänst" och är ett rent deskriptivt dokument som varken avser att ersätta relevant lagtext eller utgöra något juridiskt bindande dokument.

Nedan redogörs för förklaringen av begreppet som Kommissionen specificerar i det publicerade svardsdokumentet.

### 2 Frågeställning

Frågan som besvarats avser artikel 3.21 i DORA som behandlar definitionen av IKT-tjänster. Enligt artikeln är IKT-tjänster digitala tjänster och datatjänster som fortlöpande tillhandahålls genom IKT-system till en eller flera interna eller externa användare. Frågan som ställs är vilka typer av tjänster som bör anses vara IKT-tjänster.

### 3 Kommissionens svar

Kommissionen betonar inledningsvis att IKT-tjänster medvetet har givits en bred tillämpning. Detta framkommer av skäl 35 i DORA som klargör att för att upprätthålla en hög nivå av digital operativ motståndskraft bör definitionen förstås i bred bemärkelse, under förutsättning att sådana tjänster omfattar digitala tjänster och datatjänster som tillhandahålls fortlöpande genom IKT-system.

De finansiella entiteternas ansvar är därför att genomföra en bedömning med beaktande av denna breda tillämpning för att kunna avgöra om de tjänster som används är IKT-tjänster enligt DORA. I den bedömningen ska också skäl 63 beaktas som anger att DORA omfattar ett brett

spektrum av tredjepartsleverantörer av IKT-tjänster, inbegripet finansiella entiteter som tillhandahåller IKT-tjänster till andra finansiella entiteter.

Finansiella tjänster kan innefatta en IKT-komponent. Om finansiella entiteter tillhandahåller IKT-tjänster till andra finansiella entiteter, bör de mottagande finansiella entiteterna bedöma om:

- i) tjänsterna utgör en IKT-tjänst enligt DORA, samt
- ii) de tillhandahållande finansiella entiteterna och de finansiella tjänsterna som de tillhandahåller är reglerade enligt unionslagstiftning eller nationell lagstiftning i en medlemsstat eller i ett tredjeland.

Om svaren på både i) och ii) är "ja", ska den relaterade IKT-tjänsten anses vara en finansiell tjänst, inte en IKT-tjänst enligt artikel 3 i DORA.

Kommissionen förtydligar därtill att om tjänsten tillhandahålls av en reglerad finansiell entitet som erbjuder reglerade finansiella tjänster men är oberoende eller inte relaterad till sådana reglerade finansiella tjänster, bör tjänsten anses vara en IKT-tjänst.

Detta gäller också för hjälpande tjänster som tillhandahålls av en finansiell entitet, beroende på om de är reglerade finansiella tjänster eller tjänster som är oåtskiljbara från, förberedande eller nödvändiga för tillhandahållandet av en reglerad finansiell tjänst och inte tillhandahålls på ett fristående sätt.

#### **4 Wesslau Söderqvist Advokatbyrås rekommendationer**

Förtydligandet av skillnaden mellan finansiella tjänster och IKT-tjänster påverkar inte kraven som gäller för finansiella enheter enligt DORA, utöver kraven relaterade till hantering av risker från IKT-tredjeparter.

Förtydligandet från Kommissionen innebär att om en reglerad finansiell entitet tillhandahåller en tjänst som inte har ett direkt samband med de reglerade finansiella tjänsterna som entiteten erbjuder, eller om tjänsten är oberoende av sådana tjänster, ska den anses vara en IKT-tjänst enligt definitionen i artikel 3.21 i DORA.

Wesslau Söderqvist Advokatbyrå rekommenderar att alla tjänster som köps från en finansiell entitet ska bedömas utifrån Kommissionens tillhandahållna svar. Klassificeringen påverkar hur tjänsten regleras och vilken riskhantering som ska tillämpas enligt DORA. Den centrala frågan är alltså hur nära kopplad tjänsten är till de reglerade finansiella tjänsterna. Om kopplingen saknas eller är svag anses tjänsten falla under DORA:s definition av IKT-tjänster. Wesslau Söderqvist





Advokatbyrå rekommenderar även att slutsatserna ska dokumenteras för att ha en tydlig spårbar process för klassificeringen för att underlätta intern efterlevnad och externa revisioner eller tillsynsaktiviteter.

Oaktat om en tjänst bedöms som en finansiell tjänst, ska finansiella entiteter bedöma den IKT-risk som kan följa av avtalsförhållandet. Det kan vara risker kopplade till exempelvis incidenter som sker hos den finansiella entiteten som tillhandahåller tjänsten och hur de påverkar den egna verksamheten.

Har ni frågor med anledning av det ovanstående är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå.

## Nyhetsbrev

Ang. Hållbarhetsrisker i skadeförsäkringsföretagens Orsa-rapporter

---

21 februari 2025

### 1 Sammanfattning

Finansinspektionen har analyserat hur ett urval av skadeförsäkringsföretag har inkluderat hållbarhetsrisker i sina risk- och solvensbedömningar, nedan Orsa-rapporter, för år 2023. Analysen visar att exponeringen mot risker är påtaglig för samtliga skadeförsäkringsföretag samt att det är rapportering och analys av fysiska risker som genomgående håller högst nivå, medan analysen av andra hållbarhetsrelaterade risker varit nästintill obefintlig.

Sedan år 2022 ställs det krav på försäkringsföretag att identifiera och bedöma hållbarhetsrisker i företagsstyrningen. Därtill ska företagen beakta hållbarhetsrisker i bedömningen av det totala solvensbehovet och i Orsa-rapporterna.<sup>1</sup> I slutet av år 2024 har det införts ändringar i Solvens 2-direktivet som i Sverige ska tillämpas från den 30 januari 2027.<sup>2</sup> Härigenom kommer ett krav införas på att analysera och rapportera om klimatförändringsscenarier. I företagens identifiering och bedömning av lång- och kortsiktiga risker i Orsa-rapporterna ska det också bedömas om företaget har någon väsentlig exponering för klimatförändringsrisker. Om så är fallet ska företaget redogöra för minst två långsiktiga klimatförändringsscenarier.

Mot bakgrund av detta har Finansinspektionen formulerat kriterier för sin granskning som i korthet innebär att Orsa-rapporterna, när de nya kraven börjar gälla, ska innehålla en sammanställning av all väsentlig exponering för klimatförändringsrisker. Om klimatförändringsriskerna inte är väsentliga för företaget bör rapporten innehålla en förklaring till det.

### 2 Finansinspektionens granskning

Finansinspektionen har granskat hur skadeförsäkringsföretag med väsentlig exponering för klimatförändringsrisker har inkluderat hållbarhetsrisker i sina Orsa-rapporter. Granskningen

---

<sup>1</sup> Kommissionens delegerade förordning (EU) 2021/1256 av den 21 april 2021 om ändring av delegerad förordning (EU) 2015/35 vad gäller integrering av hållbarhetsrisker i försäkrings- och återförsäkringsföretags företagsstyrning (Solvens 2-förordningen).

<sup>2</sup> Europaparlamentets och rådets direktiv (EU) 2025/2 av den 27 november 2024 om ändring av direktiv 2009/138/EG, vad gäller proportionalitet, tillsynskvalitet, rapportering, långsiktiga garantiåtgärder, makrotillsynsverktyg, hållbarhetsrisker samt grupp-tillsyn och gränsöverskridande tillsyn, och om ändring av direktiven 2022/87/EG och 2013/34/EU (Solvens 2-förordningen).

visar att det finns betydande utrymme för förbättringar på flera centrala områden, varigenom följande områden särskilt betonas.

## **2.1 Skadeförsäkringsföretag måste utveckla sina väsentlighetsbedömningar**

Skadeförsäkringsföretagen måste utveckla sina väsentlighetsbedömningar inför att kravet på väsentlighetsbedömningar i Solvens 2-direktivet ska börja tillämpas.

Varje skadeförsäkringsföretag måste göra en väsentlighetsbedömning av klimatförändringsriskerna. Detta innebär att företaget ska identifiera de klimatförändringsrisker som företaget är exponerat för och bedöma omfattningen av denna exponering. Bedömningen ska vara både kvalitativ och kvantitativ och metoden som använts måste kunna redovisas.

Mot bakgrund av detta finner Finansinspektionen att många av företagen redogjort ytterst knapphändigt för sina väsentlighetsbedömningar och vissa av dem inte alls. Finansinspektionen betonar vikten av att arbeta vidare med väsentlighetsbedömningarna, då dessa är grundläggande för att kunna bedöma kvaliteten på och relevansen av övriga delar i Orsa-rapporterna. Därutöver påverkar väsentlighetsbedömningen helhetsbedömningen, vilket innebär att en bristande helhetsbedömning kan begränsa förståelsen för potentiella klimatrelaterade konsekvenser för företagets affärsmodell, riskprofil och solvensbehov.

## **2.2 Försäkringsföretag måste inkludera en långsiktig scenarioanalys**

Om företaget identifierar väsentliga risker ska dessa analyseras utifrån scenarioanalyser. Företag som har väsentlig exponering för klimatförändringsrisker ska ta fram minst två olika långsiktiga klimatscenarioanalyser, utöver att bedöma kortsiktig klimatpåverkan.

Granskningen visar att många försäkringsföretag behöver förbättra sin rapportering av scenarioanalyser. Trots att nästintill samtliga företag hade inkluderat scenarioanalyser i sin rapportering hade långt ifrån alla tagit med scenarier med ett långsiktigt perspektiv, i vilka ska redogöras för hur hållbarhetsrisker kan komma att påverka företagets affärsmodell på sikt.

## **3 Wesslau Söderqvist Advokatbyrås rekommendationer**

Finansinspektionen signalerar tydligt att försäkringsföretagen behöver fokusera på klimatförändringsrisker i sina Orsa-rapporter. I takt med att regelverket träder i kraft i början av år 2027 kommer Finansinspektionen att följa upp efterlevnaden av de nya reglerna i Solvens 2-direktivet.



Wesslau Söderqvist Advokatbyrå rekommenderar mot bakgrund av det som presenterats i granskningen att försäkringsföretagen ska se över och uppdatera rutinerna för Orsrapporterna avseende just klimatförändringsrisker i förhållande till försäkringsföretaget. Av särskild vikt är att analysera och redogöra för på vilket sätt företaget är exponerat för klimatförändringsrisker och i det fall väsentliga risker anses föreligga upprätta scenarioanalyser som utgår från ett långsiktigt perspektiv.

Har ni frågor med anledning av det ovanstående eller önskar stöd med det fortsatta arbetet med implementeringen av det förändrade hållbarhetsregelverket är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå.