



**Tjänsteutlåtande**

Utfärdat 2025-01-09

Ärendenummer FGL-2024-00070

Handläggare

Petra Willquist

Telefon: 031-368 5514

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

## Regelefterlevnadsfunktionens årsrapport 2024

### Förslag till beslut

I styrelsen för Försäkrings AB Göta Lejon:

Styrelsen antecknar regelefterlevnadsfunktionens årsrapport 2024.

### Sammanfattning

Regelefterlevnadsfunktionen avrapporterar den granskning som utförts i enlighet med beslutad granskningsplan. 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.

### Bedömning ur ekonomisk dimension

Kontrollfunktionens granskar bolagets följsamhet mot krav som gäller för bolagets tillståndspliktiga verksamhet. Ur ekonomiskt perspektiv är det viktigt då det är en del av att säkerställa bolagets långsiktiga ekonomiska hållbarhet.

### Bedömning ur ekologisk dimension

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

### Bedömning ur social dimension

Brister i följsamhet mot bestämmelser, regelverk och riskaptit kan leda till ökad risk för minskat förtroende för bolagets verksamhet.

### Samverkan

Ingen samverkan har genomförts.

### Bilagor

1. Årsrapport regelefterlevnadsfunktionen 2024

## Ärendet

Information till styrelsen om regelefterlevnadsfunktionens årsrapport.

För att ta del av rapporten hänvisas till bilaga 1.

## Beskrivning av ärendet

Enligt Försäkringsrörelselagen 10 kap, 4 § ska försäkringsföretag ha fyra centrala funktioner. Dessa utgörs av regelefterlevnadsfunktionen, riskhanteringsfunktionen, aktuariefunktionen och internrevisionsfunktionen. Dessa kontrollfunktioner ska utvärdera systemet för internrevision, regelefterlevnad och riskhantering. Funktionerna ska även utvärdera andra delar av företagsstyrningssystemet och rapportera resultatet och lämna rekommendationer efter utvärdering till företagets styrelse.

Regelefterlevnadsfunktionen avrapporterar den granskning som utförts i enlighet med beslutad granskningsplan.

Under första kvartalet har kontroller utförts avseende GDPR, rapportering, Återförsäkring samt övrig regelefterlevnad

Under andra kvartalet har kontroller utförts avseende outsourcing, anpassning till nya eller förändrade regelverk samt övrig regelefterlevnad.

Under tredje kvartalet har kontroller utförts avseende bolagets hantering av kunskap och kompetens hos såväl anställda som styrelsen. Därtill har funktionen för regelefterlevnad granskat bolagets hantering av intressekonflikter samt bolagets riktlinjer för ändamålet.

Under fjärde kvartalet har kontroller utförts avseende försäkringsverksamhet samt övrig regelefterlevnad.

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.

Göta Lejon arbetar löpande med att åtgärda utfärdade rekommendationer.

Rekommendationerna uppdateras i bolagets styrnings- och ledningssystem Stratsys minst två gånger per år.

## Bolagets bedömning

Det är bolagets bedömning att rapporten är relevant för bolagets arbete.

Petra Willquist

Annika Forsgren

Bolagscontroller

Vd



Till

Styrelsen i Försäkrings AB Göta Lejon

## **Rapport avseende regelefterlevnad för perioden 1 januari - 31 december 2024**

### **1 Inledning**

Styrelsen i Försäkrings AB Göta Lejon, nedan Bolaget, har uppdragit åt Wesslau Söderqvist Advokatbyrå i Stockholm KB att upprätthålla funktionen för regelefterlevnad avseende Bolagets verksamhet.

Inom ramen för uppdraget har funktionen för regelefterlevnad åtagit sig att kontrollera och regelbundet bedöma om de åtgärder och rutiner som Bolaget vidtagit för att minimera riskerna för att Bolaget inte fullgör sina förpliktelser enligt de författningar som reglerar Bolagets verksamhet är lämpliga och effektiva, utvärdera de åtgärder som vidtagits för att avhjälpa eventuella brister i Bolagets regelefterlevnad samt lämna råd och stöd till relevanta personer, så att verksamheten bedrivs i enlighet med för Bolaget gällande regelverk. Funktionen för regelefterlevnads närmare skyldigheter framgår av det avtal som träffats med Bolaget.

I avsnitt 2 nedan redovisas i sammandrag de åtgärder som funktionen för regelefterlevnad vidtagit inom ramen för ovan nämnda uppdrag under perioden 1 januari - 31 december 2024.

En översikt över utförda kontroller och eventuella synpunkter finns i [bilaga 1](#). I avsnitt 3 nedan redovisas funktionen för regelefterlevnads övergripande bedömning av Bolagets regelefterlevnad avseende den aktuella perioden.

För uppdraget ansvarar advokat Johan Grenefalk.

## **2 Händelser av relevans under året**

### **2.1 Kontroll av Bolagets regelefterlevnad**

#### **2.1.1 Kvartal 1**

##### GDPR

Uppföljning och kontroll av Bolagets personuppgiftshantering. Kontrollen har syftat till att säkerställa dels att Bolagets riktlinjer avseende personuppgiftshantering är upprättade enligt gällande regler, dels att Bolagets personuppgiftsregister är upprättat i enlighet med gällande regler.

Funktionen för regelefterlevnad har mottagit relevanta styrdokument avseende personuppgiftshantering samt Bolagets personuppgiftsregister och granskat dessa. Beträffande personuppgiftsregistret så är det under revidering och kommer att följas upp igen under år 2025.

Funktionen för regelefterlevnad anser att tidigare justeringsförslag är åtgärdade och har inte haft några synpunkter med anledning av kontrollen.

##### Rapportering

Uppföljning och kontroll av Bolagets rapportering till Finansinspektionen samt processen för ERSA-arbetet. Rapporten ska efter färdigställandet kommuniceras med Finansinspektionen.

Bolaget har redogjort för gällande rapporteringsrutiner samt att detta arbete huvudsakligen fungerar på ett bra och tillfredsställande sätt.

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

##### Övrig regelefterlevnad

Uppföljning och kontroll av Bolagets rutiner och riktlinjer avseende dels riskhantering, dels återförsäkringsrisker. Kontrollen har syftat till att dels säkerställa att Bolagets riktlinjer efterlever aktuella lagkrav, dels kontrollera huruvida dessa riktlinjer är i behov av översyn mot bakgrund av kommande regler i DORA-förordningen.

Funktionen har mottagit och granskat riktlinjerna. Riktlinjerna uppfyller väl nuvarande legala krav, men kan kräva vissa justeringar med anledning av kommande regelverk.

Funktionen för regelefterlevnad följer löpande implementeringen av DORA-förordningen i Bolagets verksamhet samt kommer även att tillstålla Bolagets styrelse en särskild plan med rekommendationer för implementeringsarbetet.

### **2.1.2 Kvartal 2**

#### Avgränsning och metod

Andra kvartalets kontroll har till övervägande del bestått i att följa upp Bolagets anpassning till den kommande DORA-förordningen, vilket innefattar flera av kontrollområdena nedan, med undantag för anpassningen till nya hållbarhetsregler samt revideringar i Solvens II-direktivet. Bolaget har tillsammans med funktionen för regelefterlevnad planerat för implementeringsarbetet avseende DORA i enlighet med den GAP-analys som Bolaget mottagit från extern leverantör. Anpassningen till nya hållbarhetsregler samt revideringar i Solvens II-direktivet har endast diskuterats med Bolaget, inga särskilda stickprov har utförts.

#### Outsourcing

Granskning av Bolagets uppdragsavtal samt Bolagets uppföljning av uppdragstagare i syfte att säkerställa att Bolaget uppfyller kraven på innehåll i sådana avtal enligt dels försäkringsrörelselagen (2010:2043) (FRL), dels Finansinspektionens föreskrifter och allmänna råd om försäkringsrörelse (FFFS 2015:8), dels Kommissionens delegerade förordning 2015/35 om upptagande och utövande av försäkringsverksamhet, dels EIOPA:s riktlinjer om uppdragsavtal med molntjänstleverantörer. Kontrollen har vidare syftat till att säkerställa att Bolaget har en fullgod uppföljning av Bolagets uppdragstagare.

Utöver ovan har även kontrollen syftat till att följa upp vilka förändringar som eventuellt behöver göras i Bolagets riktlinjer och uppdragsavtal med anledning av DORA-förordningen.

Funktionen för regelefterlevnad har inte haft några synpunkter på nuvarande utformning av avtal eller uppföljningsprocess av uppdragstagare. Funktionen har emellertid sett att vissa justeringsbehov finns för att dessa dokument och processer ska överensstämma med DORA-förordningen och kommer att hanteras mot bakgrund av den GAP-analys Bolaget mottagit under hösten.



### Anpassning till nya eller förändrade regelverk

Uppföljning och kontroll av Bolagets anpassning till dels DORA-förordningen, dels nya regler om hållbarhetsredovisning, dels omarbetningen av Solvens II. Kontrollen har syftat till att säkerställa att Bolaget har anpassat rutiner och processer efter de nya regelverken.

Beträffande anpassningen till DORA-förordningen så pågår detta arbete i enlighet med ovan. Beträffande anpassningen till de nya reglerna om hållbarhetsredovisning samt omarbetningen av Solvens II-direktivet så består dessa förändringar i nuläget i förändrade regler kring hållbarhet. Bolaget träffas inte direkt av de nämnda hållbarhetsreglerna men kommer att behöva leverera information och data till Staden som omfattas av reglerna om hållbarhetsredovisning.

Funktionen för regelefterlevnad har inte haft några synpunkter med anledning av kontrollen, men kommer fortsatt att följa och bistå i implementeringsarbetet av DORA-förordningen.

### Övrig regelefterlevnad

Uppföljning och kontroll av Bolagets riktlinjer för avbrottsfri verksamhet. Kontrollen har syftat till att säkerställa att riktlinjerna följer relevanta regler.

Funktionen har tagit del av och granskat Bolagets riktlinjer för avbrottsfri verksamhet. Funktionen för regelefterlevnad har inte haft några synpunkter på nuvarande utformning av riktlinjerna, men har emellertid sett att vissa justeringsbehov finns för att detta dokument ska överensstämma med DORA-förordningen.

## **2.1.3 Kvartal 3**

### Kontroll av Bolagets regelefterlevnad

Tredje kvartalets kontroll har till övervägande del bestått i att följa upp Bolagets hantering av kunskap och kompetens hos såväl anställda som styrelsen. Kontrollen har utgått ifrån de krav som uppställs i försäkringsrörelselagen (FRL) samt i lagen om försäkringsdistribution (LFD). Därtill har funktionen för regelefterlevnad granskat Bolagets hantering av intressekonflikter samt Bolagets riktlinjer för ändamålet.



### Intressekonflikter

Uppföljning av identifiering och hantering av intressekonflikter. Kontrollen har syftat till att följa upp om Bolaget identifierat några nya intressekonflikter som behövt hanteras.

Bolaget har redogjort för Bolagets interna rutiner för att identifiera och hantera intressekonflikter. Funktionen för regelefterlevnad har vidare tagit del av Bolagets interna riktlinjer för hantering av intressekonflikter som omfattar samtliga anställda och Bolagets ledning. Utöver att det finns en anmälningsskyldighet avseende intressekonflikter i verksamheten så är det även en stående punkt vid varje styrelsesammanträde i Bolaget. Funktionen har därtill utfört en särskild kontroll där anställda och styrelsen fått besvara frågor angående intressekonflikter samt intygat att inga sådana som kan påverka Bolaget negativt föreligger.

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

### Kunskap och kompetens hos anställda

Granskning av Bolagets interna rutiner och riktlinjer för kunskap och kompetens. Kontrollen har syftat till att säkerställa att Bolaget vidtar rimliga åtgärder för att efterleva kunskaps- och fortbildningskravet i försäkringsdistributionsregelverket (IDD).

Bolaget har redogjort för Bolagets interna rutiner för fortbildning och kunskapstest som omfattar de anställda som direkt deltar i Bolagets försäkringsdistribution. Bolaget bedöms ha goda rutiner för löpande fortbildning. Bolagets anställda har därtill avlagt godkänt kunskapstest avseende år 2024, med undantag för en person som ska utföra testet innan året är slut.

Funktionen för regelefterlevnad bedömer sammantaget att Bolaget har goda rutiner och riktlinjer för att säkerställa efterlevnad av kraven på kunskap och kompetens enligt IDD.

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

### Fit & proper

Uppföljning av styrelsens samlade kompetens. Kontrollen har syftat till att säkerställa att Bolagets styrelse efterlever kraven som ställs i Solvens II-regelverket på styrelsens samlade kompetens samt följa upp om det finns behov av kompetensutveckling.

Bolagets styrelse har under år 2024 genomfört den årliga "fit & proper"-övningen där samtliga styrelseledamöter skattat dels sin egen enskilda kunskap och kompetens, dels styrelsens samlade kompetens. I denna övning identifieras eventuella behov av kompetensutveckling och Bolaget följer upp och justerar styrelsens utbildningsplan för kommande år.

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

#### **2.1.4 Kvartal 4**

##### Försäkringsverksamhet

Kontroll av Bolagets skadereglering. Kontrollen har syftat till att säkerställa att Bolaget har ändamålsenlig skadereglering och skadehantering.

Bolaget har redogjort för Bolagets skadereglering och skadehantering samt vilka rutiner och processer som finns på plats.

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

##### Övrig regelefterlevnad

- a) Uppföljning av Bolagets organisation. Kontrollen har syftat till att följa upp eventuella förändringar i verksamheten som skulle kunna innebära någon risk i regelefterlevnadshänseende.

Bolagets organisation har diskuterats. Bolaget har under året tillsatt flera positioner som tidigare varit vakanta. Bolaget upplever att detta alltså krävt mycket arbete, men att förändringarna gett positiv effekt.

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

- b) Uppföljning av Bolagets framåtblickande bedömning av egna risker och det egna kapitalet (ORSA). Kontrollen har syftat till att säkerställa att Bolaget ser över och genomför nödvändiga uppdateringar i Bolagets ORSA för det fall detta är påkallat. Bolaget har informerat funktionen för regelefterlevnad om att scenarier i ORSA ses över regelbundet samt att styrelsen vid sammanträde i december godkände ORSA för år 2024.



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

### **2.1.5 Regelbevakning**

Under år 2024 har följande nyhetsbrev och sanktionsbeslut tillställts Bolaget. Nyhetsbrev som avser det fjärde kvartalet återfinns i sin helhet i [bilaga 2](#), medan tidigare utskick finns återgivna sedan tidigare i respektive kvartalsrapport.

#### Nyhetsbrev Q1-Q3

- Förslag till ändrade föreskrifter om åtgärder mot penningtvätt och finansiering av terrorism
- DORA, PM från Finansdepartementet
- Anmärkning och sanktionsavgift mot Loomis Sverige AB
- Vägledning för upprättande av PRIIP-faktablad för fonder
- Granskning av dataskyddsombudens roll och ställning
- Teknisk standard incidenthantering
- Kontraktsmässiga arrangemang
- IKT-säkerhet och IKT-risker
- Finansinspektionen återkallar Finans 24/7 Sverige AB:s tillstånd
- Europeiska tillsynsmyndigheterna har offentliggjort den andra omgången policyprodukter inom ramen för DORA
- Slutgiltig rapport om förslag till tekniska tillsynsstandarder och tekniska genomförandestandarder för incidentrapportering
- Finansinspektionen utfärdar sanktionsavgift på grund av överträdelse av EU:s marknadsmissbruksförordning
- Sanktionsavgifter mot Apoteket och Apohem för överföring av personuppgifter till Meta
- Finansinspektionen ingriper mot FCG Fonder AB på grund av marknadsmanipulation

## Nyhetsbrev Q4

- Finansinspektionen ger Marginalen Bank en varning
- Föreskrifter om behandling av personuppgifter som rör lagöverträdelser
- Lagrådsremiss om kompletterande lagstiftning till DORA samt förslag till föreskriftsändringar
- Antagen teknisk standard för informationsregister enligt DORA
- ESA:s beslut om tidslinje för insamling av information
- Finansinspektionens anmärkning och sanktionsavgift mot Klarna Bank AB

### **2.2 Råd och stöd**

Funktionen för regelefterlevnad har löpande under år 2024 lämnat råd och stöd till Bolaget avseende verksamheten.

### **3 Funktionen för regelefterlevnads samlade 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 9 januari 2025



Johan Grenefalk

## 1 Översikt regelefterlevnad för kvartal 4, 2024

	Område	Kontroll	Anmärkning
	Försäkringsverksamhet	Skadereglering.	Ingen anmärkning.
	Övrig regelefterlevnad	Organisation.	Ingen anmärkning.
		ERSA/ORSA.	Ingen anmärkning.

\*Denna matris syftar till att ge Bolaget en överblick över resultatet av utförd kontroll av Bolagets regelefterlevnad samt återge vilka åtgärder som Bolaget rekommenderas att vidta eller som är under arbete. Denna färgskala är inte kopplad till den riskmatris som har tillsänts Bolaget som bilaga till årsplanen.

## 2 Översikt regelefterlevnad från föregående kontroller

	Kvartal	Område	Kontroll	Anmärkning
	N/A			

\*Denna matris syftar till att ge Bolaget en överblick över föregående kontroller där funktionen för regelefterlevnad har haft anmärkingar eller synpunkter som inte är hanterade eller som är under arbete och som funktionen för regelefterlevnad avser att följa upp.

## 3 Färggradering

	Utförd kontroll har inte föranlett någon anmärkning.
	Utförd kontroll har föranlett mindre anmärkning eller synpunkt. Åtgärd rekommenderas eller är under arbete.
	Sannolikhet för att regelavvikelse inträffar. Åtgärd behöver vidtas inom kort.
	Regelavvikelse har uppmärksamats vid utförd kontroll. Åtgärd behöver vidtas snarast.

## Nyhetsbrev

Ang. Lagrådsremiss om kompletterande lagstiftning till DORA samt förslag till föreskriftsändringar

---

3 oktober 2024

### 1 Inledning

I augusti har en lagrådsremiss om digital operativ motståndskraft för finanssektorn publicerats. Kraven i DORA omfattar bl.a. riskhantering när det gäller informations- och kommunikationsteknik, nedan IKT, incidentrapportering, hantering av utlagd verksamhet och testning av digital operativ motståndskraft. DORA kräver vissa nationella lagstiftningsåtgärder. I den publicerade lagrådsremissen föreslås därför en ny lag med kompletterande bestämmelser till DORA som bl.a. reglerar Finansinspektionens tillsynsbefogenheter, ingripanden och sanktioner. Därutöver föreslås ändringar i flera näringsrättsliga regleringar. I tillägg till detta har Finansinspektionen den 4 september 2024 även publicerat förslag till justeringar i allmänna råd och föreskrifter.

Den nya lagen och övriga lagändringar i näringsrättslig reglering föreslås träda i kraft den 17 januari 2025, dvs. samma datum som DORA ska börja tillämpas. Finansinspektionen föreslår även att de nya och ändrade föreskrifterna och allmänna råden ska träda i kraft samma datum.

Observera att det som anges nedan är förslag och att det inte finns något slutligt beslut avseende de föreslagna bestämmelserna i lag eller föreskrifter.

### 2 Ny lag som kompletterar DORA

Den nya kompletterande lagen till DORA innebär bl.a. följande.

- Det befästs att Finansinspektionen blir tillsynsmyndighet och att Finansinspektionen ska kunna förelägga fysiska och juridiska personer att inkomma med uppgifter. Finansinspektionen ska också kunna genomföra platsundersökningar.
- Finansinspektionen ska (i viss samverkan med Riksbanken) kunna besluta om vilka finansiella entiteter som ska genomföra hotbildsstyrda penetrationstester. Finansinspektionen ska också kunna besluta om hur ofta en finansiell entitet ska genomföra sådana tester. Riksbanken ska kunna utfärda intyg som bekräftar att genomförda test uppfyller kraven i DORA.

- Finansiella entiteter får en uppgiftsskyldighet till Riksbanken i syfte att Riksbanken ska kunna övervaka och samordna hotbildstyrda penetrationstester.

### **3 Finansinspektionens nya föreskrifter om rapportering av informationsregister och allvarliga IKT-incidenter**

Nya föreskriftsbestämmelser införs för samtliga finansiella entiteter som omfattas av DORA. Dessa bestämmelser innebär följande.

- Incidenter: Finansiella entiteter ska rapportera *allvarliga* IKT-relaterade incidenter till Finansinspektionen på det sätt som anges på Finansinspektionens webbplats. Samma format kommer att tillämpas för frivillig anmälan av betydande cyberhot.
- Informationsregister: Finansiella entiteter ska varje år skicka in sitt informationsregister till Finansinspektionens på det sätt som anges på Finansinspektionens webbplats. Rapporteringen av informationsregister ska ha kommit in till Finansinspektionen senast den 28 februari varje år och gälla förhållandena vid utgången av föregående kalenderår.

Det ovanstående innebär att det första rapporteringstillfället för informationsregistret är den 28 februari 2025 avseende uppgifter per den 31 januari 2025. De föreslagna tidpunkterna för rapportering kan komma att justeras, eftersom det ännu inte är känt vilka tidpunkter som kommer att gälla för Finansinspektionens vidare rapportering av uppgifter till de europeiska tillsynsmyndigheterna.

### **4 Ingripanden mot finansiella entiteter och fysiska personer**

Finansinspektionen har, genom gällande bestämmelser i rörelselagarna, de befogenheter att ingripa mot finansiella entiteter som krävs enligt DORA. Finansinspektionens möjligheter att ingripa genom föreläggande att vidta rättelse, genom förbud att verkställa beslut, genom anmärkning samt beslut om att återkalla tillstånd eller meddela varning kvarstår. Förelägganden och förbud kan förenas med vite. Vid anmärkning och varning kan sanktionsavgifter påföras.

Finansinspektionen ska få ingripa mot någon som ingår i styrelsen för finansiella entiteter eller är dess vd, eller ersättare för någon av dem, om den finansiella entiteten har åsidosatt sina skyldigheter enligt DORA. För finansiella entiteter som är AIF-förvaltare ska detta också gälla förvaltarens *ledning* eller vd eller motsvarande (med anledning av att AIF-förvaltare får bedriva verksamhet i andra former än aktiebolag, t.ex. handelsbolag).

Ett ingripande ska endast få ske om den finansiella entitetens överträdelse är allvarlig och den fysiska personen i fråga uppsåtligt eller av grov oaktsamhet orsakat överträdelsen. I detta

ligger att företrädaren har en betydande del i överträdelsen och, genom sin ställning, har haft möjlighet att agera för att förhindra överträdelsen. Ingripande ska få ske genom en eller båda av följande administrativa sanktioner:

- 1) att den fysiska personen under en viss tid, lägst tre och högst tio år, inte får företräda den finansiella entiteten, eller
- 2) sanktionsavgift.

Ett beslut om förbud mot att företräda den finansiella entiteten ska få förenas med vite. Bestämmelserna om ingripanden kommer att införas i rörelseregleringen.

Sanktionsavgiften för en fysisk person ska som högst kunna fastställas till det högsta av:

- 1) ett belopp motsvarande 500 000 euro, eller
- 2) tre gånger den vinst som den fysiska personen har gjort till följd av regelöverträdelsen, om beloppet går att fastställa.

## **5 Allmänna råd om händelser av väsentlig betydelse**

Finansinspektionens allmänna råd (FFFS 2021:2) om rapportering av händelser av väsentlig betydelse ändras genom att den incidentrapportering som ska ske enligt DORA inte ska omfattas av FFFS 2021:2. Därför lämnas nya allmänna råd om rapportering av händelser av väsentlig betydelse vars tillämpningsområde inte omfattar incidentrapportering enligt DORA. Dessa allmänna råd gäller inte för bl.a. försäkringsföretag och värdepappersföretag. För dessa företag införs dock samma justeringar i de specifika föreskrifterna som ska tillämpas av de företagen, se nedan.

## **6 Krav på nätverks- och informationssystem**

I och med DORA införs nya krav på finansiella entiteters riskhantering. Finansiella entiteter ska vidta de åtgärder som är nödvändiga för att de ska kunna bedriva sin verksamhet och tillhandahålla tjänster och därigenom garantera en smidigt fungerande inre marknad. Därmed förtydligas i de olika rörelselagarna kraven på nätverks- och informationssystem som blir mer detaljerade eftersom rutinerna för bl.a. drift och förvaltning av dessa system ska uppfylla de krav som närmare anges i DORA.

## 7 Övriga justeringar i rörelselagar och befintliga föreskrifter

### 7.1 Bank- och finansieringsrörelse

I Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:4) om hantering av operativa risker införs följande föreskriftsändringar.

- Bestämmelserna i föreskrifterna ska inte gälla för hantering av sådana IKT-risker som avses i DORA. Begränsningen införs för att undvika dubbelreglering och tydliggöra att hanteringen av IKT-risker ska ske enligt DORA. Föreskrifterna om operativa risker ska alltså gälla för hantering av andra operativa risker än IKT-risker.
- Bestämmelserna om identifiering och mätning, process för godkännande och utseende av person för att hantera risker i samband med nyheter ska inte längre gälla för IT-system.
- Upplysningsbestämmelsen om bestämmelserna om informationssäkerhet, bestämmelsen om IT-system och bestämmelsen om huvudsakligt IT-driftställe ska upphöra att gälla eftersom Finansinspektionen föreslår att 2 och 3 kap. i FFFS 2014:5 ska upphöra att gälla för att undvika dubbelreglering, se nedan.

I Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:5) om informationssäkerhet, IT-verksamhet och insättningssystem införs följande föreskriftsändringar.

- DORA innehåller bestämmelser om informationssäkerhet och IT-verksamhet. Sådana bestämmelser finns även i kommissionens delegerade förordning (EU) 2024/1774. FFFS 2014:5 upphävs därför för att undvika dubbelreglering och ersätts av nya allmänna råd om insättningssystem. Bestämmelserna i FFFS 2014:5 om informationssäkerhet och IT-verksamhet förs alltså inte över till de nya föreskrifterna. Inte heller de bestämmelser om insättningssystem som tar sikte på IT-system förs över till de nya föreskrifterna. Övriga bestämmelser om insättningssystem i IT-föreskrifterna förs över till de nya föreskrifterna.

### 7.2 Fondförvaltare (UCITS)

I Finansinspektionens föreskrifter (FFFS 2013:9) om värdepappersfonder införs följande föreskriftsändringar.

- I verksamhetsplanen ska det lämnas en redogörelse för hur fondbolaget säkerställer att fondbolaget uppfyller DORA:s bestämmelser om hantering av IKT-tredjepartsrisker.
- Bestämmelserna om rapportering av händelser av väsentlig betydelse ska inte gälla för incidentrapportering enligt DORA. För rapportering av andra händelser av väsentlig betydelse än de som omfattas av DORA ska 10 kap. FFFS 2013:9 alltså tillämpas.

- Bestämmelserna om uppdragsavtal ska inte gälla för hantering av IKT-tredjepartsrisker enligt DORA för att undvika dubbelreglering. För andra uppdragsavtal än de som omfattas av DORA ska 14 kap. FFFS 2013:9 alltså tillämpas.
- Bestämmelsen om att fondbolag ska ha aktuella system och rutiner för att skydda säkerhet, integritet och konfidentialitet i sin information upphävs eftersom det finns motsvarande bestämmelser i DORA som ska efterlevas av fondbolag.

### **7.3 AIF-förvaltare**

I Finansinspektionens föreskrifter (FFFS 2013:10) om förvaltare av alternativa investeringsfonder införs följande föreskriftsändringar.

- Redogörelsen för uppdragsavtal i en AIF-förvaltares verksamhetsplan ska innehålla uppgifter om hur förvaltaren säkerställer att denne uppfyller kraven på uppdragsavtal enligt DORA.
- I verksamhetsplanen ska AIF-förvaltaren även beskriva hur förvaltaren uppfyller de krav som följer av DORA när det gäller organisation av IT-verksamheten.

### **7.4 Värdepappersinstitut**

I lagen (2007:528) om värdepappersmarknaden införs följande bestämmelser.

- Ett värdepappersinstitut ska ha sunda skyddsmekanismer för att i enlighet med kraven i DORA säkerställa skyddet och autentiseringen vid informationsöverföring och för att minimera risken för dataförvanskning och obehörig åtkomst till informationen.
- Ett värdepappersinstitut ska ha inrättat effektiva arrangemang för kontinuerlig drift av verksamheten för att hantera driftavbrott i sina handelssystem, inbegripet en IKT-kontinuitetspolicy och IKT-kontinuitetsplaner samt IKT-relaterade åtgärds- och återställningsplaner. Institutet ska se till att systemen är fullt testade och lämpligt övervakade för att säkerställa att de uppfyller kraven i DORA samt bestämmelserna om ingripanden mot fysiska personer som är styrelseledamöter eller vd, eller ersättare för någon av dem.

I Finansinspektionens föreskrifter (FFFS 2007:17) om verksamhet på marknadsplatser införs följande föreskriftsändringar.

- Ett företag ska i sin verksamhetsplan särskilt ange hur företaget ska följa DORA. Det ska också finnas en beskrivning av sådana arrangemang, planer, förfaranden och mekanismer





som företaget har fastställt för att säkerställa att information om allvarliga IKT-relaterade incidenter och betydande cyberhot överförs till Finansinspektionen.

## **8 Wesslau Söderqvist Advokatbyrås rekommendationer**

Informationsregistret över IKT-tjänster ska rapporteras till Finansinspektionen för första gången den 28 februari 2025. Finansinspektionen har per dagens datum inte angett på vilket sätt som informationsregistret ska skickas in. Advokatbyrån rekommenderar ändå att finansiella entiteter ska ta fram de uppgifter som kommer att behöva anmälas in i enlighet med EBA:s *Draft Technical Standards to establish the templates for the register of information*. Registret är tämligen omfattande och kommer troligen kräva att uppgifter behöver begäras in från IKT-tjänsteleverantörerna. Finansinspektionen kommer att tillhandahålla ett gränssnitt för inrapporteringen och finansiella entiteter måste säkerställa att de har ett sådant gränssnitt som krävs för att kunna överföra informationen till Finansinspektionen. Arbetet bör påbörjas omgående för att säkerställa att rapportering av registret kan ske den 28 februari 2025.

Advokatbyrån rekommenderar också att finansiella aktörer i god tid ska säkerställa att rutinerna för rapportering av allvarliga incidenter är ändamålsenliga och från och med den 17 januari 2025 kan möta rapporteringskraven enligt DORA. Sådant rapportering ska genomföras så snabbt som möjligt inom fyra timmar från att en incident klassificerats som *allvarlig* men inte senare än 24 timmar från upptäckt.

Utöver de områden som nämns ovan rekommenderar Advokatbyrån att det bl.a. genomförs utbildningsinsatser för att öka medvetenheten kring informationssäkerhet i hela organisationen.

Har ni frågor med anledning av det ovanstående eller har behov av hjälp med att implementera DORA är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå.

## Nyhetsbrev

Ang. Finansinspektionen ger Marginalen Bank en varning

---

17 oktober 2024

### 1 Finansinspektionens varning

Finansinspektionen, har den 16 oktober 2024 utfärdat en varning mot Marginalen Bank, nedan Banken, för överträdelse av reglerna om stora exponeringar och kraven på god riskhantering.

Finansinspektionen har granskat Bankens exponeringar mot fyra bolag, nedan Bolagen, under perioden 30 september 2021 - 30 september 2023 och anser att Bolagen har haft sådana kopplingar till varandra att de utgör en grupp av kunder med inbördes anknytning i enlighet med tillsynsförordningen<sup>1</sup>. Enligt tillsynsförordningen ska de totala exponeringarna mot en sådan grupp beräknas genom att exponeringarna mot de enskilda kunderna i gruppen läggs samman. Bankens exponering mot en grupp av kunder med inbördes anknytning får i sin tur sammantaget inte överstiga 25 procent av Bankens primärkapital.

Finansinspektionen konstaterar att Banken har underlåtit att lägga samman den totala exponeringen för Bolagen med inbördes anknytning, vilket rätteligen skulle ha gjorts. I enlighet med de siffror som Banken har rapporterat till Finansinspektionen framgår det att Bankens totala exponeringar mot Bolagen har uppgått till cirka 77 procent av Bankens primärkapital den 30 september 2023. År 2022 har exponeringarna uppgått till drygt 57 procent och år 2021 har de uppgått till cirka 30 procent. Eftersom Bankens totala exponeringar mot Bolagen överstigit gränsvärdet om 25 procent konstaterar Finansinspektionen att Banken under en tvåårsperiod har haft exponeringar som överstigit gränsen för vad som är tillåtet. Med anledning härav bedömer Finansinspektionen att Banken har brustit i sin riskhantering.

Finansinspektionen anför att tillsynsförordningens bestämmelser om kreditinstituts maximala exponeringar är nära sammankopplade med riskhanteringsreglerna i LBF<sup>2</sup>. Enligt dessa regler ska ett institut upprätthålla adekvata system för att identifiera, värdera och hantera sina risker, med hänsyn till verksamhetens art, omfattning och komplexitet. Finansinspektionen anser att Bankens agerande har resulterat i långvariga exponeringar som väsentligt överstigit de tillåtna

---

<sup>1</sup> Europaparlamentets och rådets förordning (EU) nr 575/2013 av den 26 juni 2013 om tillsynskrav för kreditinstitut och värdepappersföretag och om ändring av förordning (EU) nr 648/2012.

<sup>2</sup> Lag (2004:297) om bank- och finansieringsrörelse.



gränsvärdena, vilket inneburit att Banken utsatt sig för en oacceptabelt hög förlustrisk och äventyrat sin finansiella stabilitet.

## **2 Wesslau Söderqvist Advokatbyrås rekommendationer**

En välfungerande riskhantering är en grundläggande förutsättning för att kreditinstitut ska kunna bedriva sin verksamhet på ett sunt och regelbundet sätt. Wesslau Söderqvist Advokatbyrå rekommenderar att kreditinstituten säkerställer att dess exponering är förenlig med tillsynsförordningen. Vid bedömningen av den tillåtna gränsen för exponering ska särskild hänsyn tas till kunder som har sådana kopplingar till varandra att de kan utgöra en grupp av kunder med inbördes anknytning enligt tillsynsförordningens mening. Så kan vara fallet om antingen en av kunderna utövar direkt eller indirekt kontroll över de andra, eller om det finns en sannolikhet för att ekonomiska problem hos en kund påverkar även den andra kunden. Om det föreligger omständigheter som pekar mot sådana förbindelser bör kreditinstitutet lägga ihop sina exponeringar mot dessa kunder.

Wesslau Söderqvist Advokatbyrå rekommenderar även att finansiella institut i allmänhet mot bakgrund av Finansinspektionens beslut ska se över sina exponeringar och koncentrationsrisker samt rutiner och processer hänförliga till hanteringen av risker för att undvika likartade fallissemang.

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



WESSLAU SÖDERQVIST

## Nyhetsbrev

Ang. Föreskrifter om behandling av personuppgifter som rör lagöverträdelser

---

4 november 2024

### 1 Nya föreskrifter från IMY förenklar kontroll mot sanktionslistor

Från och med den 1 november 2024 har nya föreskrifter från Integritetsskyddsmyndigheten (IMY) trätt i kraft som gör det enklare för företag att utföra kontroller mot sanktionslistor.<sup>1</sup> Företag som står under Finansinspektionens tillsyn kommer inte längre att behöva ansöka om tillstånd från IMY för att kontrollera sina kunder mot sanktionslistor.

En av förutsättningarna för att få utföra dessa kontroller är att behandlingen är nödvändig. För att behandling av personuppgifter ska anses nödvändig behöver emellertid inte regelverken uttryckligen kräva kontroller mot sanktionslistor. Nödvändighetsrekvisitet anses exempelvis uppfyllt för en bank som behandlar personuppgifter som rör lagöverträdelser i syfte att säkerställa efterlevnaden av kraven på kundkännedom enligt lagen om åtgärder mot penningtvätt och finansiering av terrorism.

Vidare förutsättningar för att få utföra dessa kontroller är att sanktionslistorna är fastställda i demokratisk ordning och allmänt tillgängliga på de utfärdande myndigheternas eller mellanstatliga organisationernas webbplatser. Detta innebär att listor som företag eller koncerner själva har skapat internt inte omfattas av de nya föreskrifterna.

Vid kontroller mot sanktionslistor ska även integritetsskyddande åtgärder vidtas i syfte att säkerställa att eventuella träffar som uppstår vid kontrollerna är äkta. En sådan åtgärd kan vara att ha rutiner som säkerställer att den person som finns upptagen på en sanktionslista och som ett företag får träff på vid kontroll mot sanktionslistan utgör den person som företaget avsett att kontrollera, exempelvis en person som företaget avser att ingå en affärsförbindelse med.

Förutsättningarna i sin helhet återges i IMY:s författningssamling IMYFS 2024:1.

### 2 Wesslau Söderqvist Advokatbyrås rekommendationer

Trots att ansökan inte längre görs gällande, rekommenderar Wesslau Söderqvist Advokatbyrå att aktörer beaktar den kvarstående skyldigheten att följa gällande regelverk vid genomförandet

---

<sup>1</sup> Se *Vägledning – föreskrifter om behandling av personuppgifter som rör lagöverträdelser (IMYFS 2024:1)*.



av kontroller mot sanktionslistor. Behandlingen av personuppgifter måste fortfarande bedömas som nödvändig för att uppfylla de rättsliga kraven för personuppgiftsbehandling. Vidare bör det säkerställas att eventuella träffar som uppstår vid kontroller är korrekta och avser den person som företaget faktiskt avsett att kontrollera.

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



## Nyhetsbrev

Ang. ESA:s beslut om tidslinje för insamling av information

---

18 november 2024

### 1 Bakgrund

Från och med nästa år ska finansiella aktörer i enlighet med DORA rapportera in sina informationsregister om kontraktsmässiga arrangemang med IKT-tredjepartsleverantörer till Finansinspektionen. Rapporteringen baseras på det utkast till tekniska standarder (ITS) som publicerades av de europeiska tillsynsmyndigheterna i januari 2024. EU-kommissionen avvisade i september utkastet till ITS om informationsregister på grund av att IKT-tredjepartsleverantörer skulle behöva identifieras med en LEI-kod (Legal Entity Identifier). EU-kommissionen anser att det bör vara möjligt att välja mellan att använda LEI-kod eller EUID (European Unique Identifier) för att identifiera IKT-tredjepartsleverantörer. I sitt svar till EU-kommissionen pekar EBA, Esma och Eiopa på vilka utmaningar de ser med att inkludera EUID i informationsregistren. Kontentan av detta är att ITS om informationsregister ännu inte är antagen.

Enligt DORA ska finansiella aktörer rapportera informationsregistret till Finansinspektionen den 28 februari varje år. Tidpunkten för den första rapporteringen 2025 är dock oklar med anledning av att de tekniska standarderna ännu inte är antagna.

### 2 ESA:s beslut om tidslinjen för rapportering

Från och med DORA:s ikraftträdande den 17 januari 2025 kommer ESA, tillsammans med behöriga myndigheter, att påbörja tillsynen av kritiska tredjepartsleverantörer som tillhandahåller IKT-tjänster till finansiella företag inom EU. Den första tillsynsåtgärden är att utse vilka dessa kritiska tredjepartsleverantörer är. För att kunna utse dessa måste först informationsregistren rapporteras in till tillsynsmyndigheterna, vilket även uttalades vid FI-forum den 6 november 2024.

ESA publicerade den 15 november 2024 ett beslut om vilken information som behöriga myndigheter i Europa måste rapportera för att utse kritiska tredjeparter inom informations- och kommunikationsteknik (IKT) enligt DORA. Beslutet innebär att Finansinspektionen senast den 30 april 2025 måste rapportera register över finansiella företags avtalsarrangemang med



tredjeparter inom IKT. Eftersom sista datumet för den första inlämningen av informationsregistren till ESA är satt till den 30 april 2025, förväntar sig ESA att behöriga myndigheter samlar in informationsregistren från de finansiella företagen de övervakar i förväg, enligt sina egna tidsplaner. Detta innebär därmed att finansiella aktörer kommer att behöva anmäla in informationsregistret till Finansinspektionen **innan den 30 april 2025**.

### **3 Förberedelser inför registerinlämning**

Trots att de genomförande tekniska standarderna för informationsregister ännu inte har antagits av EU-kommissionen uppmuntrar ESA finansiella aktörer att i största möjliga mån förbereda sina register.

ESA:s utkast till mall över registret finns tillgängligt här:

[RegisterInformationTemplatesIllustration \(1\).xlsx](#)

Q&A som tagits fram efter den frivilliga testrapporteringen av informationsregister finns här:

[DORA Dry Run FAQ \(Updated\).pdf](#)

ESA har även publicerat en lista över valideringsregler som kommer att användas vid analys av informationsregister samt en visuell representation av datamodellen. Dessa regler kommer att inkluderas i det uppdaterade tekniska rapporteringspaketet som ska publiceras i december 2024. Valideringsreglerna finns här: [Draft validation rules for DORA reporting of RoI.xlsx](#)

### **4 Wesslau Söderqvist Advokatbyrås kommentarer**

Informationsregistret som ska rapporteras till Finansinspektionen är tämligen omfattande. Rapporteringen ska göras via Finansinspektionens webbplats där Finansinspektionen kommer att tillhandahålla gränssnitt för den inrapportering som ska göras. Även om det ännu inte är klarlagt vid vilken tidpunkt eller hur rapporteringen ska göras, rekommenderar Advokatbyrån att arbete påbörjas för att fylla i informationsregistret utifrån den mall som tillhandahålls i dagsläget. Även om EU-kommissionen och EBA, Esmå och Eiopa för en diskussion om att inkludera EUID, bedöms förändringar från det förslag som finns publicerat idag som begränsade.

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



## Nyhetsbrev

Ang. antagen teknisk standard för informationsregister enligt DORA

---

6 december 2024

### 1 Sammanfattning

EU-kommissionen har antagit den genomförandeförordning<sup>1</sup> som fastställer innehållet och utformningen av informationsregistret som ska rapporteras till Finansinspektionen enligt DORA. Registret ska innehålla information – på enhets- och koncernnivå – om IKT-avtal och tredjepartsleverantörer av IKT-tjänster. Tidigare under hösten har ett utkast till informationsregistret avisats på grund av att IKT-tredjepartsleverantörer enligt förslaget behövt identifieras med en LEI-kod. Enligt den nu antagna standarden kan tredjepartsleverantörer av IKT-tjänster identifieras med antingen LEI-kod eller EUID, eller båda dessa.

Finansiella entiteter ska använda mallarna i bilagorna I till IV till genomförandeförordningen när informationsregistret upprätthålls och uppdateras. Uppgiftslämnandet ska följa principerna för bland annat korrekthet, fullständighet och enhetlighet.

### 2 Informationsregistret

#### 2.1 Innehåll

I genomförandeförordningen specificeras vilken information som de finansiella entiteterna måste inkludera i informationsregistret. På ett övergripande plan ska informationsregistret innehålla uppgifter om följande.

- Allmän information om den finansiella entiteten som för registret samt om koncernen och filialer,
- allmän och specifik information om avtalsarrangemang,
- information om tredjepartsleverantörer av IKT-tjänster,
- information om leveranskedjan och underleverantörer,
- identifieringskoder och funktioner,
- bedömning av kritiska IKT-tjänster, samt
- terminologi och klassificeringssystem.

---

<sup>1</sup> Kommissionens genomförandeförordning (EU) 2024/2956.



## 2.2 Typer av IKT-tjänster

I informationsregistret ska de finansiella entiteterna ange de aktuella typerna av IKT-tjänster. I bilaga III till genomförandeförordningen specificeras och beskrivs de olika typerna av IKT-tjänster, vilket även kan ge ledning för finansiella entiteter att identifiera vilka IKT-tjänster som används. Några exempel på IKT-tjänster är tillhandahållande av data, dataanalys, programvaru-licensiering, tillhandahållande av hårdvara och fysiska enheter som arbetsstationer och telefoner.

## 2.3 Format för inrapportering

Av genomförandeförordningen framgår att alla mallar som utgör informationsregistret ska vara tabeller med ett förbestämt antal kolumner och obegränsat antal rader. Bilagorna till genomförandeförordningen utgör ett informationsunderlag för upprättandet av registret men dessa är inte utformade som färdiga ifyllnadsbara mallar. Finansinspektionen har dock förklarat att myndigheten kommer att tillhandahålla ett gränssnitt för den inrapportering som ska göras (FI dnr 1341). Detta gränssnitt har inte publicerats ännu.

Enligt nuvarande förslag från Finansinspektionen ska informationsregistret inrapporteras den 28 februari varje år och gälla förhållandena vid utgången av föregående kalenderår. Det första rapporteringstillfället kommer dock att vara den 15 april 2025 och då avse förhållandena vid utgången av mars 2025.

## 3 Resurs- och tidsåtgång

Finansinspektionen har uppskattat företagens kostnader för att säkerställa att de har ett sådant gränssnitt som krävs för att kunna överföra informationen till Finansinspektionen.

Anpassningen av IT-system som kan behöva göras av företagen är en engångskostnad som kan variera beroende på vilken lösning som företagen har och om arbetet utförs av egen personal eller av konsulter. I denna del uppskattas tidsåtgången för arbetet till 40 - 80 timmar och kostnaden till 60 000 - 160 000 kronor per företag. Observera att detta endast är en uppskattning.

Företagen kan även behöva göra Anpassningar i sina rapporteringsrutiner i samband med att informationsregistret ska inrapporteras vilket uppskattas bestå i en engångskostnad motsvarande en arbetsinsats om cirka 10 - 20 timmar. Därutöver behöver företagen senast den 28 februari varje år – med undantag för förtä rapporteringstillfället – säkerställa att uppgifterna

förs över till Finansinspektionen i en samlad rapport. Att granska och skicka in uppgifterna uppskattas motsvara en årlig arbetsinsats om ca 10 – 20 timmar.

Finansinspektionen framhåller dock att det i beräkningen inte ingår kostnader för att initialt upprätta och därefter uppdatera informationsregistret. Kostnaden för detta kan variera beroende på antalet och omfattningen av de kontraktsrättsliga arrangemangen.

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

Genomförandeförordningen fastställer vad informationsregistret ska innehålla men det återstår att se vilket format som ska användas vid själva inrapporteringen. Det är tänkbart att den gemensamma mallen som EBA upprättat tidigare kommer att tillhandahållas för rapporteringen. I väntan på att formerna för rapporteringen kommer på plats rekommenderar Wesslau Söderqvist Advokatbyrå att finansiella entiteter påbörjar arbetet med att ta fram informationen som ska finnas med i registret enligt den mall som nu finns publicerad. Vidare bör berörda företag se över om ytterligare IKT-tjänster kan identifieras efter förtydligandet i genomförandeförordningen. Observera att skälen i DORA anger att definitionen av IKT-tjänster bör omfatta t.ex. s.k. over-the-top-tjänster, som omfattas av kategorin elektroniska kommunikationstjänster. Definitionen bör endast utsluta den begränsade kategori av traditionella analoga telefonitjänster som räknas som tjänster inom det allmänna telefonnätet (PSTN), tjänster inom fasta nät, konventionella telefontjänster (POTS) eller telefonitjänster inom fasta nät.

Första rapporteringstillfället är den 15 april 2025. Wesslau Söderqvist Advokatbyrå rekommenderar att arbetet med informationsregistret påbörjas omgående mot bakgrund av den omfattande informationsinhämtning som rapporteringen kommer att innebära.

Om ni har frågor med anledning av implementeringen av DORA, eller behöver hjälp med informationsregistret enligt den nya genomförandeförordningen är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå.



## Nyhetsbrev

Ang. Finansinspektionen utfärdar anmärkning och sanktionsavgift mot Klarna Bank AB på grund av överträdelse av penningtvättsregelverket

---

11 december 2024

### 1 Sammanfattning

Finansinspektionen har funnit att Klarna Bank AB, nedan Klarna, har åsidosatt penningtvättsregelverket på flera grunder. Bland annat har det saknats riskbedömningar avseende hur bankens produkter och tjänster kan utnyttjas för penningtvätt eller finansiering av terrorism. Därutöver har det saknats riktlinjer för kundkännedom, särskilt rutiner och riktlinjer som fångar upp situationer när kundkännedomsåtgärder ska vidtas. Mot den bakgrunden har Finansinspektionen beslutat att utfärda en anmärkning och en sanktionsavgift på 500 miljoner kronor.

### 2 Bakgrund och Finansinspektionens ärende

Klarna har tillstånd att driva bankrörelse enligt lagen (2004:297) om bank- och finansieringsrörelse. Klarna erbjuder bland annat en kassalösning till e-handlare som innebär att konsumenter kan välja när och hur de vill betala för varor och tjänster. Genom dessa betalningsmetoder kan väljas att betala direkt, genom faktura eller avbetalning.

Finansinspektionen inledde i april 2022 en undersökning av Klarna. Syftet var att granska hur penningtvättsregelverkets bestämmelser om allmän riskbedömning och rutiner och riktlinjer för kundkännedomsåtgärder genomfördes.

Penningtvättsregelverket syftar till att förhindra att verksamhetsutövare utnyttjas för penningtvätt och finansiering av terrorism. Utgångspunkten är ett riskbaserat förhållningssätt, vilket innebär att en verksamhetsutövare ska vidta åtgärder som står i proportion till de risker för penningtvätt och finansiering av terrorism som den är exponerad för.

Enligt regelverket ska verksamhetsutövaren göra en allmän riskbedömning för att bedöma hur de produkter och tjänster som tillhandahålls kan utnyttjas för penningtvätt och finansiering av terrorism. Därutöver ska verksamhetsutövaren ha dokumenterade rutiner och riktlinjer för sina åtgärder för kundkännedom.

### **3 Finansinspektionens iakttagelser och bedömningar**

#### **3.1 Den allmänna riskbedömningen**

Finansinspektionen framhåller att Klarnas allmänna riskbedömning beskriver egenskaperna hos de produkter och tjänster som Klarna tillhandahåller på ett övergripande sätt. Det redovisas också för hur stora riskerna är för att produkterna och tjänsterna kan utnyttjas för penningtvätt eller finansiering av terrorism. Bristen som dock särskilt uppmärksammas är bedömningen av hur stor risken är för att ett utnyttjande sker i den specifika verksamheten. Trots att Klarna tar upp olika omständigheter i den allmänna riskbedömningen går de inte vidare med att göra en bedömning av hur omständigheterna bidrar till att just de produkter och tjänster som tillhandahålls kan utnyttjas för penningtvätt eller finansiering av terrorism.

Därtill uppmärksammas brister i beaktandet av risker förknippade med Klarnas distributionskanaler. Eftersom Klarna har en särskild handlartyp; betaltjänstleverantörer som i sin tur har en stock av andra handlare, föreligger risk för penningtvätt och finansiering av terrorism. Den ifrågasatt strukturen kallas "mor-modellen" vilken genererade 12,2 procent av Klarnas totala inkomst från handlarna under granskningsperioden. Finansinspektionen konstaterar att mor-handlarna, mot Klarnas förnekande, kategoriseras som distributörer och därför ingår i en sådan distributionskanal som ska beaktas vid den allmänna riskbedömningen.

Finansinspektionen finner slutligen brister i analysen av de misstankerapporter som nämns i den allmänna riskbedömningen. Klarna har vidare inte gjort någon egentlig bedömning av de risker som identifierats i allmänhet, varför riskbedömningen inte kan anses kunna ligga till grund för Klarnas rutiner, riktlinjer och övriga åtgärder vilket krävs enligt penningtvättsregelverket.

#### **3.2 Rutiner och riktlinjer för kundkännedomsgärder**

I centrum för granskningen av Klarnas kundkännedomsgärder har frågan varit om konsumenter som använder produkten "faktura" är att ses som kunder i penningtvättslagens mening. Avgörande är om konsumenterna har trätt i, eller står i begrepp att träda i, avtalsförbindelse med Klarna.

Konsumenter som vill använda någon av Klarnas betalningsmetoder måste registrera sig och godkänna Klarnas villkor, varigenom konsumenten ingår ett avtal med Klarna genom att acceptera villkoren. Mot bakgrund av att godkännandet är ett grundläggande krav för att kunna använda Klarnas betalningsmetoder bedömer Finansinspektionen att konsumenterna är kunder

i penningtvättslagens mening. Därför har rutiner och riktlinjer för kundkännedomsgärder varit påkallade, vilka brustit i verksamheten.

Finansinspektionen uppmärksammar att kravet på kundkännedomsgärder inom affärsmässiga förbindelser inte uppstår direkt då kunden för första gången ingår avtal om att använda produkten faktura. För att en sådan förbindelse ska etableras krävs att kunden också använder någon av Klarnas produkter vid flera tillfällen. Klarna har saknat rutiner och riktlinjer för situationer där kundkännedomsgärder måste vidtas gällande sådana affärsförbindelser.

Avseende transaktioner som inte utförs inom ramen för en affärsförbindelse ska åtgärder för kundkännedom vidtas vid transaktioner som understiger ett belopp om 15 000 euro och som verksamhetsutövaren inser eller borde inse har samband med en eller flera andra transaktioner och som tillsammans uppgår till minst detta belopp. För att fånga upp dessa transaktioner har Klarna kategoriserat transaktioner utförda inom tolv månader som sådana. Finansinspektionen konstaterar att flera än den omständigheten kan tyda på ett sådant samband varigenom Klarna konstateras ha saknat de rutiner och riktlinjer som krävs.

### **3.3 Finansinspektionens ingripande**

Klarnas agerande har inneburit överträdelser av centrala bestämmelser i penningtvättslagen under en längre tid. Däremot har inte överträdelserna lett till några skador eller konkreta effekter på det finansiella systemet, förutom potentiella effekter genom att bristerna inneburit att riskerna för utnyttjande har ökat. Finansinspektionen ger Klarna en anmärkning som tillsammans med en sanktionsavgift om 500 miljoner kronor anses tillräckligt ingripande.

## **4 Wesslau Söderqvist Advokatbyrås rekommendationer**

Den allmänna riskbedömningen ska anpassas till den egna verksamheten. Särskilt ska beaktas vilka slags produkter och tjänster som tillhandahålls, vilka kunder och distributionskanaler som finns och vilka geografiska riskfaktorer som föreligger. Beslutet visar på vikten av att ha en process för att identifiera vilka som är "kunder" i penningtvättslagens mening.

Wesslau Söderqvist Advokatbyrå rekommenderar att aktörer som omfattas av penningtvättsregelverket kontrollerar sin allmänna riskbedömning för att säkerställa att en heltäckande analys av företagets verksamhet har gjorts. I verksamheten måste, exempelvis, tas ställning till om betaltjänstleverantörer är att se som led i en distributionskanal. I det fallet ska



betaltjänstleverantörerna analyseras i den allmänna riskbedömningen för att se om det finns risk för att produkterna och tjänsterna utnyttjas för penningtvätt eller finansiering av terrorism.

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

## Nyhetsbrev

Ang. Anmärkning och en sanktionsavgift mot Partner Fondkommission AB för överträdelse av reglerna om transaktionsrapportering

---

13 december 2024

### 1 Sammanfattning

Finansinspektionen har funnit att värdepappersbolaget Partner Fondkommission AB, nedan Partner, i samband med att bolaget medverkat vid sju riktade nyemissioner har brutit i sin grundläggande skyldighet att transaktionsrapportera till Finansinspektionen. Genom att underlåta detta har Partner åsidosatt kraven i artikel 26.1 i förordningen om marknader för finansiella instrument (Mifir). Partner har till följd av överträdelsen fått en anmärkning och ska betala en sanktionsavgift om 100 000 kronor.

### 2 Bakgrund och Finansinspektionens ärende

Partner är ett värdepappersbolag som bl.a. har tillstånd att utföra order på kunders uppdrag enligt lagen (2007:528) om värdepappersmarknaden (Vpml). Partner erbjuder bl.a. finansiell rådgivning och emissionstjänster, t.ex. genom att i samband med en nyemission upprätta marknadsföringsmaterial, kontakta investerare, hantera teckningslistor och teckningssedlar samt ta emot emissionslikvider från investerare för emittenters räkning.

I den löpande tillsynen har Finansinspektionen uppmärksammat att Partner vid en riktad nyemission inte rapporterat några utförda transaktioner. Detta har medfört att Finansinspektionen inlett en undersökning i februari 2024 för att undersöka huruvida Partner hade fullgjort sin skyldighet att rapportera utförda transaktioner med finansiella instrument i enlighet med artikel 26.1 i Mifir.

### 3 Rättsliga utgångspunkter

Värdepappersbolag som utför transaktioner med finansiella instrument är enligt artikel 26.1 i Mifir skyldiga att så snart som möjligt, och senast i slutet av nästa arbetsdag, lämna fullständiga och korrekta uppgifter om transaktionerna till den behöriga myndigheten.

Rapporteringskyldigheten gäller oberoende av om transaktionerna har utförts på handelsplatsen eller inte. Vad som utgör en transaktion fastställs i artikel 2 i kommissionens delegerade förordning (EU) 2017/590. Av artikel 2.1 i den delegerade förordningen framgår

det att slutförandet av ett förvärv, eller en avyttring av ett sådant finansiellt instrument som avses i artikel 26.2 i Mifir, anses utgöra en transaktion. Enligt artikel 2.2 a och 2.3 a ska begreppen förvärv och avyttring innefatta köp och försäljning av finansiella instrument.

#### **4 Finansinspektionens bedömning och ingripande**

Investerings tjänsten att "utföra order på kundens uppdrag" enligt Vpml, skiljer sig något från definitionen av sådan tjänst enligt Mifir. Finansinspektionen har dock konstaterat att det av förarbetena till regleringen framgår att någon saklig skillnad inte är avsedd. Den investeringstjänst som Partner har tillstånd för motsvarar således samma tjänst som avses i artikel 3.1 b i den delegerade förordningen 2017/590, dvs. exekvera order för kunds räkning. Den omständigheten att ordet "exekvera" används i den delegerade förordningen i stället för "utföra" förändrar inte detta, utan begreppen är synonyma i sammanhanget. Vid tidpunkten för respektive emission har alla emittenternas finansiella instrument handlats på en multilateral handelsplattform, vilket inneburit att emissionerna rört sådana instrument som omfattas av rapporteringsskyldigheten. Partner har vid emissionerna haft varierande uppgifter. Vid vissa emissioner har Partner haft i uppdrag att utföra samtliga moment, bl.a. att göra marknadssonderingar och kontakta investerare som i sin tur tecknat sig i emissionerna. Vid andra emissioner har Partner fungerat som finansiell rådgivare till emittenten och i vissa fall har Partner delat uppdraget med ett annat företag.

Finansinspektionen bedömer att Partners tillhandahållande av investeringstjänsten har lett till transaktioner vid samtliga av emissionerna och att tjänsterna har utgjort transaktioner i enlighet med artikel 26.1 i Mifir. Följden är att Partner varit skyldigt att transaktionsrapportera vid ett drygt hundratal transaktioner. Genom att underlåta att rapportera har Partner överträtt bestämmelserna i artikel 26.1 i Mifir.

Finansinspektionen bedömer att överträdelserna har varit sådana att det finns skäl att ingripa mot Partner. Överträdelserna har dock inte varit så allvarliga att det finns skäl att återkalla Partners tillstånd eller ge bolaget en varning. Finansinspektionen har därför beslutat att ge Partner en anmärkning i förening med en sanktionsavgift om 100 000 kronor.

#### **5 Wesslau Söderqvist Advokatbyrås rekommendationer**

Sanktionsbeslutet har relevans särskilt för värdepappersbolag med tillstånd enligt Vpml. En väl fungerande transaktionsrapportering är en grundläggande förutsättning för en effektiv marknadsövervakning, vilket ökar Finansinspektionens möjlighet att upptäcka och utreda marknadsmissbruk.





Mot bakgrund av Finansinspektionens beslut framhävs vikten av att utreda om det vid handel med finansiella instrument finns en skyldighet att transaktionsrapportera eller om det finns en tydlig gräns mot andra, inte rapporteringsskyldiga, aktiviteter som exempelvis att lämna rådgivning om transaktionsstrukturen. Wesslau Söderqvist Advokatbyrå rekommenderar därför att rapporteringspliktiga bolag ser över sina rutiner för rapportering och säkerställer att det finns riktlinjer på plats för vilka uppdrag som utgör transaktioner med finansiella instrument och vilka som faller utanför. Samma rekommendation gäller för övriga finansiella aktörer som av en eller annan anledning är rapporteringspliktiga till Finansinspektionen, att se över att rätt information når Finansinspektionen inom utsatt tid.

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

## Nyhetsbrev

Ang. Finansinspektionens föreskrifter och allmänna råd till följd av Dora-förordningen

---

20 december 2024

### 1 Sammanfattning

Finansinspektionen, nedan FI, har beslutat om nya och ändrade föreskrifter och allmänna råd till följd av EU:s förordning om digital operativ motståndskraft för finanssektorn, nedan Dora. Eftersom Dora gäller för de flesta typer av företag under FI:s tillsyn har ändringar genomförts i flera föreskrifter som gäller för olika delar av finanssektorn. För att undvika dubbelreglering har även delar av tidigare föreskrifter upphävts.

FI har även beslutat om nya föreskrifter där det anges vilket tekniskt format som företagen ska använda vid rapporteringen, samt vid vilken tidpunkt som de ska rapportera in informationsregister enligt Dora.

De nya och ändrade föreskrifterna och allmänna råden träder i kraft den 17 januari 2025.

### 2 Rapportering av incidenter och informationsregister

FI har antagit nya föreskrifter om rapportering av incidenter och informationsregister enligt Dora (FFFS 2024:20). Föreskrifterna är kortfattade och anger att allvarliga IKT-relaterade incidenter ska rapporteras till FI på det sätt som anges på FI:s webbplats. Detsamma gäller för sådan frivillig rapportering av betydande cyberhot som avses i Dora. Rapporteringen kommer att genomföras i rapporteringssystemet Fidac genom att använda mallarna som har tagits fram av de europeiska tillsynsmyndigheterna.

De finansiella entiteterna ska ge FI tillgång till sitt fullständiga register med information om kontraktsmässiga arrangemang och lämna in detta till FI senast den 15 april 2025 och därefter senast den 28 februari varje år. Den version av registret som lämnas in ska avse förhållandena vid utgången av föregående kalenderår. Det första rapporteringstillfället ska dock avse förhållandena vid utgången av mars 2025. Företagen ska rapportera in informationsregistret på det sätt som anges på FI:s webbplats.

### **3 Allmänna råd om rapportering av händelser av väsentlig betydelse**

FI har beslutat om ändringar i allmänna råd om rapportering av väsentlig betydelse (FFFS 2024:22). De allmänna råden gäller inte för rapportering av IKT-relaterade incidenter enligt artikel 19 i Dora. Enligt de nya allmänna råden bör företag rapportera händelser som kan medföra att dess ekonomiska förutsättningar ändras eller som kan äventyra deras förmåga att uppfylla sina åtaganden mot kunder. Företagen bör därför rapportera händelser som kan medföra att ett större antal kunder orsakas betydande ekonomisk skada eller en väsentlig ryktesförlust för företaget. Det kan till exempel vara om kundtransaktioner hanteras på ett felaktigt sätt eller om fel uppstår i tekniska system.

### **4 Verksamhetspecifika föreskrifter**

FI har även beslutat om ändringar i flera föreskrifter för att anpassa dessa till Dora.

Bland annat uppställs i värdepappersföreskrifterna krav på att fondbolag i sin verksamhetsplan ska redogöra för hur det säkerställer att det uppfyller bestämmelserna i Dora om hantering av IKT-tredjepartsrisker (Kapitel V). Bestämmelsen om att ett fondbolag ska ha aktuella system och rutiner för att skydda säkerhet, integritet och konfidentialitet i sin information upphävs. Vidare ska bestämmelserna i föreskrifterna om rapportering av händelser av väsentlig betydelse inte gälla för incidentrapportering enligt artikel 19 i Dora. Bestämmelserna om uppdragsavtal i 14 kap. i föreskrifterna ska inte heller gälla för sådana uppdragsavtal som rör hantering av IKT-tredjepartsrisker enligt Dora.

Vidare har ändringar i AIF-förvaltarföreskrifterna genomförts, vari framgår att redogörelsen för uppdragsavtal i en AIF-förvaltares verksamhetsplan även ska innehålla uppgifter om hur förvaltaren säkerställer att den uppfyller kraven på uppdragsavtal i Dora. I verksamhetsplanen ska en AIF-förvaltare därutöver beskriva hur AIF-förvaltaren uppfyller de krav som följer av Dora när det gäller organisation av it-verksamheten.

### **5 Wesslau Söderqvist Advokatbyrås rekommendationer**

När Dora ska börja tillämpas ställs skärpta krav på det förebyggande arbetet beträffande informations- och kommunikationsteknik, men även krav kopplat till avtalsparter och underleverantörer. Wesslau Söderqvist Advokatbyrå rekommenderar därför att företag som omfattas av Dora ser över vilka åtgärder som behöver vidtas inför att Dora ska börja tillämpas. Vidare kan dessa företag redan nu börja förbereda informationsregistret som ska rapporteras in till FI i april 2025. Slutligen bör företag ta del av FI:s ändringsföreskrifter som är relevanta för



den specifika verksamheten i syfte att identifiera på vilket sätt interna rutiner och styrdokument kan behöva anpassas för att leva upp till de regulatoriska kraven.

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