Till
Styrelsen i S:t Erik Försäkrings AB

Rapport för perioden 1 januari - 20 februari 2024 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.

- Förslag till ändrade föreskrifter om åtgärder mot penningtvätt och finansiering av terrorism
- Digital operativ motståndskraft för finanssektorn.

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.

Område	*Kontroll*	*Compliancerisk (Grön/Gul/Röd)*
Personuppgiftsbehandling (GDPR)	Hantering av personuppgifter samt interna rutiner och riktlinjer.	Kontrollen har inte föranlett några synpunkter.
Rapportering	Rapportering till Finansinspektionen.	Kontrollen har inte föranlett några synpunkter.
Övrig regelefterlevnad	Efterlevnad av regler för riskhantering.	Kontrollen har inte föranlett några synpunkter.
Återförsäkring	Efterlevnad av reglerna om återförsäkringsrisker m.m.	Kontrollen har inte föranlett några synpunkter.

Personuppgiftsbehandling

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.

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

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

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.

Återförsäkring

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 den stundande oberoende kontrollen och översynen som ska göras avseende återförsäkringsprogrammet, självrisker och självbehåll.

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

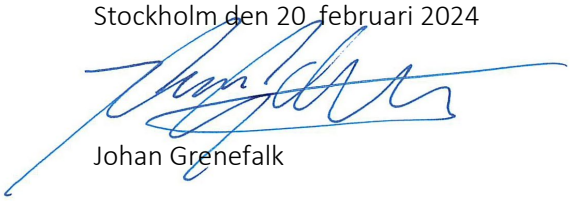
2.3 Råd och stöd

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 20 februari 2024



Johan Grenefalk

Bilaga 1

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. Förslag till ändrade föreskrifter om åtgärder mot penningtvätt och finansiering av terrorism

---

12 januari 2024

1 Bakgrund

Den 21 december 2023 har Finansinspektionen publicerat ett förslag till ändringar i Finansinspektionens föreskrifter (FFFS 2017:11) om åtgärder mot penningtvätt och finansiering av terrorism. Målet med ändringarna är att skapa en mer flexibel och ändamålsenlig reglering som tillåter enskilda näringsidkare och mindre företag, med ett begränsat antal anställda och en verksamhet som är förknippad med låg risk för penningtvätt och finansiering av terrorism, att avstå från att utse en centralt funktionsansvarig.

Företag som inte utser en centralt funktionsansvarig bör i stället säkerställa att det finns en funktion för regelefterlevnad som ansvarar för att företagets skyldigheter enligt penningtvättsregelverket genomförs och verkställs i verksamheten. Det föreslås även att i de fall det finns en centralt funktionsansvarig ska denne regelbundet, och minst årligen, rapportera om företagets arbete mot penningtvätt och finansiering av terrorism.

Dessa ändringar ligger i linje med, och bygger i stor utsträckning på, EBA:s riktlinjer.[1] Ändringarna föreslås träda i kraft den 26 mars 2024. Nedan redogörs närmare för förslaget samt dess påverkan på företag som omfattas av föreskrifterna.

2 Finansinspektionens förslag

2.1 Det ska inte vara obligatoriskt att utse en centralt funktionsansvarig

Finansinspektionen föreslår att kravet på att varje företag, enligt penningtvättsföreskrifterna, ska utse en centralt funktionsansvarig tas bort. I stället bör företag endast behöva utse en centralt funktionsansvarig om det är motiverat med hänsyn till verksamhetens storlek och art. Detta innebär att mindre företag och enskilda näringsidkare med låg risk för penningtvätt och finansiering av terrorism inte längre ska vara tvungna att utse en centralt funktionsansvarig. Förslaget grundas på de svårigheter det kan innebära för mindre företag med få anställda att anställa ytterligare en person enbart för att uppfylla detta krav . Finansinspektionen menar att

[1] *EBA:s riktlinjer i enlighet med artikel 8 och kapitel VI i direktiv (EU) 2015/849 om riktlinjer och förfaranden för efterlevnadskontroll och rollen och ansvarsområdena för den regelefterlevnadsansvarige för bekämpning av penningtvätt och finansiering av terrorism (EBA/GL/2022/05)*

den föreslagna förändringen skulle göra regleringen mer flexibel och anpassningsbar, i linje med EBA:s riktlinjer. Förslaget innebär således att det obligatoriska kravet som nu finns i 6 kap. 5 § första stycket penningtvättsföreskrifterna tas bort och att 6 kap. 1 § första stycket ändras för att inkludera bedömningen av om företag behöver utse en centralt funktionsansvarig.

2.2 Om företag inte utser en centralt funktionsansvarig

Finansinspektionen föreslår att ett företag som inte utser en centralt funktionsansvarig enligt ovan ska i stället ha en funktion för regelefterlevnad. Funktionen för regelefterlevnad ska kontrollera att företaget uppfyller sina skyldigheter enligt penningtvättsregelverket och avrapportera misstänkta fall av penningtvätt, finansiering av terrorism eller brottsligt förvärv till Polismyndigheten. Även detta är i linje med EBA:s riktlinjer.

Förslaget är inspirerat av Länsstyrelsen i Stockholms läns föreskrifter[2] och säkerställer att företaget har interna rutiner och riktlinjer för att hantera identifierade risker enligt penningtvättsregelverket även utan en centralt funktionsansvarig.

2.3 Funktionerna för intern kontroll ska framgå av företagets rutiner och riktlinjer

Finansinspektionen föreslår att ett företags rutiner och riktlinjer tydligt ska ange vilka funktioner företaget har inrättat och vilka personer som innehar dessa funktioner. Det är särskilt viktigt att klargöra vem som ansvarar för företagets rapportering till Polismyndigheten vid misstanke om penningtvätt, finansiering av terrorism eller annat brottsligt förvärv. Eftersom penningtvättsregelverket är riskbaserat och inte detaljerat reglerar vilka åtgärder som ett företag bör vidta betonas behovet för företag att själva genomföra riskbedömningar och utforma rutiner och riktlinjer i enlighet med identifierade risker.

Finansinspektionen anser att kraven på rutiner för intern kontroll i penningtvättsföreskrifterna bör kompletteras med en bestämmelse som kräver dokumentation av vilka funktioner som har inrättats och vilka personer som har dessa funktioner. Denna dokumentation ska tydliggöra ansvarsfördelningen inom företaget, underlätta beslutsprocesser och bidra till att säkerställa företagets överensstämmelse med regelverket för penningtvätt och finansiering av terrorism.

2.4 Centralt funktionsansvarig ska upprätta en rapport om företagets arbete mot penningtvätt

Finansinspektionen anser att den centralt funktionsansvariges roll vid kontroll och bedömning bör preciseras. Finansinspektionen föreslår att det bör anges att en centralt funktionsansvarig

[2] *6 kap. 3 § Länsstyrelsen i Stockholms läns föreskrifter och allmänna råd (01FS 2019:53).*

regelbundet, och åtminstone årligen, ska upprätta en rapport om företagets arbete mot penningtvätt och finansiering av terrorism. Detta ska underlätta för företagets ledning att hålla sig underrättad samt att fatta rätt beslut. Det är dessutom i linje med EBA:s riktlinjer att en sådan rapport upprättas minst årligen.

2.5 Möjlighet att uppdra åt annan att utföra en centralt funktionsansvarigs uppgifter

Det finns i dagens regelverk inte någon möjlighet att uppdra åt någon annan att utföra de uppgifter som åligger en centralt funktionsansvarig. Finansinspektionen menar att genom att tillåta att vissa av den centralt funktionsansvariges uppgifter utförs av någon utanför företaget så skapas en möjlighet för mindre företag att säkerställa att uppgifterna utförs av någon med rätt kompetens. Finansinspektionen föreslår därför att det bör vara tillåtet att uppdra åt annan att utföra dessa uppgifter.

Finansinspektionen redogör emellertid för undantag då det inte bör vara möjligt att uppdra åt annan att utföra dessa uppgifter. För det första konstaterar Finansinspektionen att det inte ska vara möjligt att placera en centralt funktionsansvarig utanför företaget. Att placera uppgifter utanför företaget bör för det andra inte avse uppgiften att rapportera misstänkta transaktioner till Polismyndigheten eller Säkerhetspolisen. Det bör för det tredje vara förenligt med den rörelsereglering som gäller för företaget i fråga att lämna ut sådant uppdrag till en person utanför företaget.[3]

3 Wesslau Söderqvist Advokatbyrås rekommendationer

Wesslau Söderqvist Advokatbyrå rekommenderar företag att redan nu se över sitt behov av en centralt funktionsansvarig med hänsyn till verksamhetens storlek och art. För det fall slutsatsen är att det inte är motiverat att utse en centralt funktionsansvarig bör företag överväga att, efter riktlinjernas ikraftträdande, se till att utvärdera vilken typ av uppgifter som i stället bör ligga på funktionen för regelefterlevnad som säkerställer att företaget uppfyller sina åtaganden att motverka penningtvätt samt rapportera misstänkta fall till Polismyndigheten.

Efter riktlinjernas ikraftträdande är det även viktigt att företag förtydligar i sina rutiner och riktlinjer vilka funktioner som finns och vilka personer som ansvarar för dem. Detta inkluderar tydliggörande av ansvar för rapportering till Polismyndigheten vid misstanke om penningtvätt, finansiering av terrorism eller brottsligt förvärv.

---

[3] *Se till exempel för kreditinstitutens del 6 kap. 7 § lagen (2004:297) om bank och finansieringsrörelse och 10 kap. Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:1) om styrning, riskhantering och kontroll i kreditinstitut.*

Om företag har en centralt funktionsansvarig rekommenderar Wesslau Söderqvist Advokatbyrå att företagen redan nu förbereder verksamheten på att regelbundet, minst årligen, vara beredd att upprätta en rapport om företagets arbete mot penningtvätt och finansiering av terrorism.

Till sist kan möjligheten att uppdra åt en extern person att utföra vissa uppgifter som normalt åligger en centralt funktionsansvarig övervägas. Funktionen som sådan kan dock inte outsourcas till extern part. Även detta är något som företag kan se över redan innan riktlinjerna träder i kraft för att vara förberedd när de väl ska tillämpas.

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

Nyhetsbrev

Ang. Digital operativ motståndskraft för finanssektorn

---

30 januari 2024

1 Bakgrund

Wesslau Söderqvist Advokatbyrå har tidigare informerat om förordningen om digital operativ motståndskraft i den finansiella sektorn, nedan DORA, som ska börja tillämpas den 17 januari 2025. Finansdepartementet har nyligen publicerat en promemoria med förslag till en ny lag med bestämmelser som ska komplettera DORA. Den nya lagen och ändringarna i näringsrättslig reglering föreslås träda i kraft samma datum som DORA. Nedan redogörs för de huvudsakliga delarna i förslaget.

2 Förslaget

2.1 IKT-relaterade incidenter och cyberhot

I DORA ges medlemsstater ett utrymme att bestämma vad som ska gälla för rapportering av IKT-relaterade incidenter och frivillig anmälan av cyberhot. Medlemsstater ges även ett utrymme att fastställa om finansiella entiteter som rapporterar frivilligt får vidarebefordra en anmälan till de CSIRT-enheter som utsetts eller inrättats i enlighet med NIS2-direktivet.

I förslaget framhålls att det är av särskild vikt att relevanta myndigheter informeras om allvarliga IKT-relaterade incidenter och betydande cyberhot så snart det är möjligt. För finansiella entiteter är det Finansinspektionen, som tillsynsmyndighet, som ska få informationen. Finansinspektionen ska i sin tur skyndsamt lämna över informationen till den myndighet eller CSIRT-enhet som inrättats enligt NIS2-direktivet. I promemorian föreslås att Sverige inte bör utnyttja mallarna i DORA för att reglera vilken information som ska lämnas till behörig myndighet eller CSIRT-enhet enligt NIS2-direktivet.

Det föreslås även att möjligheten att införa en bestämmelse där finansiella entiteter som frivilligt rapporterar om allvarligt cyberhot dessutom får vidarebefordra anmälan till den enligt NIS2-direktivet utsedda myndigheten inte ska utnyttjas.

2.2 Hotbildsstyrda penetrationstester

I promemorian föreslås att Finansinspektionen ska få bestämma vilka finansiella entiteter som ska genomföra hotbildsstyrda penetrationstester och hur ofta dessa tester ska ske. Det är

Riksbanken som ska övervaka och samordna de hotbildsstyrda penetrationstesterna. Riksbanken ska även utfärda intyg om att testerna uppfyller de krav som uppställs i DORA-förordningen.

Finansinspektionen och Riksbanken ska samarbeta bl.a. genom att Riksbanken ska få möjlighet att yttra sig innan Finansinspektionen fattar beslut om vilka finansiella entiteter som ska genomföra hotbildsstyrda penetrationstester. Vice versa bör Finansinspektionen beredas möjlighet att yttra sig innan Riksbanken fattar beslut som påverkar Finansinspektionens tillsynsverksamhet.

2.3 Tillsyn

Finansinspektionen ska enligt förslaget ha tillsyn över att finansiella entiteter följer DORA och den föreslagna kompletteringslagen. Tillsynen ska omfatta att Finansinspektionen kan förelägga en fysisk eller juridisk person att tillhandahålla uppgifter, handlingar eller annat. Finansinspektionen föreslås även få rätt att utföra platsundersökningar om det är nödvändigt.

2.3.1 Ingripanden mot finansiella aktörer

I promemorian föreslås inte några bestämmelser innebärande straffansvar för överträdelser av DORA. Däremot föreslås ingripanden mot finansiella aktörer som helhet samt för vissa företrädare av dessa.

Förslaget är att den kompletterande lagen till DORA bör inkludera en bestämmelse som informerar om att regler för åtgärder vid överträdelser av DORA återfinns i de lagar som styr finansiella aktörers verksamhet.

2.3.2 Ingripanden mot fysiska personer som företrädare för finansiella entiteter

Även vad gäller ingripande mot vissa företrädare för finansiella aktörer finns idag bestämmelser i rörelselagarna på finansmarknadsområdet. Finansinspektionens möjlighet att ingripa i dessa fall är dock begränsad till överträdelser av lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism eller rörelselagarna.

Finansinspektionen ska få ingripa mot någon i styrelsen eller vd för en finansiell aktör. Det ska även omfatta ersättare för dessa. Ingripandet ska kunna ske om någon av dessa personer har åsidosatt sina skyldigheter enligt DORA. Det ska krävas att den finansiella aktörens överträdelse är allvarlig och att den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen. Ingripandet kan resultera i två olika administrativa sanktioner, eller de båda i förening. Antingen får den fysiska personen en sanktion som innebär att personen, under lägst

tre men högst tio år, inte får vara styrelseledamot, vd eller ersättare för någon av dem. Den andra möjliga sanktionen är en sanktionsavgift.

3 Wesslau Söderqvist Advokatbyrås rekommendationer

Wesslau Söderqvist Advokatbyrå rekommenderar fortsatt att finansiella aktörer säkerställer att tillräckliga skyddsåtgärder vidtas i syfte att efterleva DORA och minska risken för IKT-incidenter. Det är viktigt att uppdatera och revidera interna rutiner, policys och riktlinjer för att spegla kompletteringslagens och DORA:s krav. Finansiella aktörer bör vidare se till att det finns tydliga processer för att följa upp och reagera på eventuella förelägganden från tillsynsmyndigheten.

Mot bakgrund av att fysiska personer som företrädare för finansiella entiteter kan åläggas sanktioner bör det i organisationen vara tydligt vilket ansvar som ledningen har för att efterleva DORA. Roller och ansvarsområden ska utryckas tydligt i interna riktlinjer på området.

Wesslau Söderqvist Advokatbyrå vill understryka vikten av att öka medvetenheten inom hela organisationen om cybersäkerhet och efterlevnaden av reglerna.

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