Göteborgs Stad

Tjänsteutlåtande
Utfärdat: 2024-11-06
Diarienummer 0013/24

Handläggare:
Petra Willquist
Telefon: 031-368 55 14
E-post: petra.willquist@gotalejon.goteborg.se

Rapport regelefterlevnadsfunktion kvartal 3 2024

Förslag till beslut

I styrelsen för Försäkrings AB Göta Lejon:

Styrelsen antecknar rapport från regelefterlevnadsfunktionen kvartal 3 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. Rapport regelefterlevnadsfunktionen kvartal 3 2024

Ärendet
Information till styrelsen om regelefterlevnadsfunktionens rapport från kvartal 3 2024.

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 tredje kvartalet har kontroller utförts avseende 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.

Under kvartal 3 2024 har regelefterlevnadsfunktionen utförda kontroller inte föranlett någon anmärkning för bolaget. 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. Göta Lejon arbetar löpande med uppföljning av rekommendationer.

Till
Styrelsen i Försäkrings AB Göta Lejon

Kvartalsrapport för perioden 1 juli - 30 september 2024 avseende regelefterlevnad

1 Inledning

Genom denna rapport återkopplar funktionen för regelefterlevnad resultatet av senast genomförd kontroll av Försäkrings AB Göta Lejons, nedan Bolaget, regelefterlevnad samt redogör för de övriga åtgärder som funktionen för regelefterlevnad har vidtagit under det tredje kvartalet 2024.

För en överblick över utfallet av kvartalets utförda kontroller, se bilaga 1.

2 Händelser av relevans under perioden

2.1 Regelbevakning

Följande nyhetsbrev har tillställts Bolaget under årets tredje kvartal. Dessa finns återgivna i sin helhet i bilaga 2.

- Anmärkning och sanktionsavgift mot Loomis Sverige AB.
- Vägledning för upprättande av PRIIP-faktablad för fonder.
- Granskning av dataskyddsombudens roll och ställning.
- Teknisk standard om 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.

2.2 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 besvarar 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.

2.3 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 31 oktober 2024

Johan Grenefalk

1 Översikt regelefterlevnad för kvartal 3, 2024

	Område	*Kontroll*	*Anmärkning*
	Övrig regelefterlevnad	Intressekonflikter.	*Ingen anmärkning*
		Kompetens och kunskapsnivå hos personalen (IDD).	*Ingen anmärkning*
		Kompetens och kunskapsnivå hos styrelsen (fit & proper) inkl. samlad kompetens.	*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*

*Denna matris syftar till att ge Bolaget en överblick över föregående kontroller där funktionen för regelefterlevnad har haft anmärkningar 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 uppmärksammats vid utförd kontroll. Åtgärd behöver vidtas snarast.

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. Anmärkning och sanktionsavgift mot Loomis Sverige AB

---

1 juli 2024

1 Bakgrund

Finansinspektionen har i sin tillsyn av bevakningsföretaget Loomis Sverige AB, nedan Loomis alternativt bolaget, identifierat flera överträdelser av centrala delar av penningtvättsregelverket. Bristerna har identifierats i verksamhetens allmänna riskbedömning, i riskbedömningen av kunder samt i de grundläggande åtgärderna för kundkännedom. Med anledning av överträdelserna tilldelas Loomis en anmärkning och åläggs att betala en sanktionsavgift om 40 miljoner kronor.

Finansinspektionen inledde en undersökning mot Loomis i april 2022. Loomis bedriver huvudsakligen värdetransportrörelse, uppräkningsverksamhet och valutaväxlingsverksamhet. Mot bakgrund av att bolaget bedriver uppräkningsverksamhet, vilket innebär att bolaget erbjuder en betaltjänst som möjliggör insättningar av kontanter på betalkonton, bedöms risken för att verksamheten utnyttjas för penningtvätt som hög. Detta medför krav på att bolaget vidtar särskilt kraftfulla åtgärder. I sin tillsyn har Finansinspektionen granskat Loomis allmänna riskbedömningar, rutiner och riktlinjer för kundkännedomsåtgärder samt riskbedömningar av kunder under perioden 1 april 2021–31 mars 2022.

2 Finansinspektionens iakttagelser i sin tillsyn

2.1 Allmän riskbedömning

Vid den allmänna riskbedömningen ska särskilt beaktas vilka slags produkter och tjänster som tillhandahålls, vilka kunder och distributionskanaler som finns och vilka geografiska riskfaktorer som föreligger. Av de kundakter som ingått i Finansinspektionens granskning framgår att Loomis har haft fyra utländska banker som möjliggjort en kontantinsättning som motsvarat cirka 20 procent av bolagets totala betalningsvolym. Finansinspektionen noterar att riskbedömningen visserligen har innefattat en bedömning av geografiska risker förknippade med olika länder. Däremot saknades en bedömning av hur riskerna som var förknippade med de länder där de utländska bankerna var etablerade påverkade risken för att Loomis tjänst skulle kunna utnyttjas. Finansinspektionen noterade därför att Loomis brustit i sin bedömning av geografiska risker.

Den allmänna riskbedömningen måste därtill avse risker som kunderna är förknippade med, särskilt i de fall kunder driver kontantintensiv verksamhet. Av Loomis allmänna riskbedömning framgick att kunder med en kontantomsättning på minst tolv miljoner kronor ansågs ha en hög omsättning av kontanter, oavsett andelen kontakta betalningar som kunderna genomfört. I detta sammanhang betonar Finansinspektionen att riskbedömningen ska utgå från de verkliga riskerna samt att verksamhetsutövare ska identifiera vilka kunder som driver kontantintensiv verksamhet för att därefter kunna bedöma riskerna som är förknippade med dem. Loomis riskbedömning avseende kunder anses otillräcklig baserat på att de beloppsgränser som bolaget angav i den allmänna riskbedömningen inte sattes i relation till exempelvis kundernas totala omsättning, eller något annat förhållande.

2.2 Riskbedömning av kunder

Verksamhetsutövare måste vidare bedöma den risk för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen. Loomis använder en modell för riskbedömning av kunder som utgår från den information som finns tillgänglig om kunden och där varje typ av information som påverkar kundens riskklass benämns riskparameter. I beslutet identifierar Finansinspektionen att Loomis inte har utgått från några specifika uppgifter om förekomsten av kontanter i kundernas verksamhet utan att endast kundernas branschtillhörighet enligt SNI-koder beaktats. Visserligen krävs inte alltid att en individualiserad bedömning av kundens riskprofil görs men mot bakgrund av att Loomis erbjuder en tjänst som innebär hög risk för penningtvätt bedömer Finansinspektionen att det varit helt nödvändigt med en individualiserad bedömning av om kunderna driver kontantintensiv verksamhet.

2.3 Åtgärder för kundkännedom

Finansinspektionen betonar att det är en grundläggande åtgärd för kundkännedom att inhämta uppgifter om affärsförbindelsens syfte och art. I det fall risken som kan förknippas med kundrelationen bedöms som hög, ska särskilda åtgärder vidtas i form av kontroller, bedömningar och utredningar. I beslutet identifieras att Loomis inte inhämtat några sådana uppgifter från en tredjedel av kunderna och endast i ytterst begränsad utsträckning från övriga kunder. Trots att insättningstjänsten inte är komplicerad är risken för att den utnyttjas hög. För att kunna göra en tillfredställande riskbedömning av kunderna och för att kunna bedöma hur de kan förväntas agera inom ramen för affärsförbindelserna skulle Loomis ha behövt inhämta mer omfattande uppgifter om affärsförbindelsernas syfte och art.

För de kunder som verksamheter bedömt vara förknippade med hög risk aktualiseras skärpta kundkännedomsåtgärder för att öka kunskapen om kunden och möjliggöra för mer välgrundade bedömningar av de transaktioner som kunden genomför. Finansinspektionen identifierar att Loomis inte inhämtat uppgifter om varifrån kundens medel kommer från majoriteten av kunderna som bolaget bedömt vara högriskkunder. Oaktat att inhämtandet av sådana uppgifter endast är exempel på en kundkännedomsåtgärd som kan vidtas, menar Finansinspektionen att det är en åtgärd som normalt måste vidtas för att få tillräcklig kunskap om kunden.

3 Finansinspektionens bedömning

Mot bakgrund av ovan nämna brister fastställer Finansinspektionen att Loomis har överträtt centrala bestämmelser i penningtvättslagen under en inte kortvarig tid. Eftersom riskerna för penningtvätt är särskilt höga i kontantintensiva företag ställs höga krav på sådana företag att vidta kraftfulla åtgärder för att förhindra att de kan utnyttjas för kriminella syften. Att en allmän riskbedömning är utformad på det sätt som regelverket kräver och att dess riskbedömning av kunder sker på ett korrekt sätt utifrån tillräckliga kundkännedomsuppgifter är helt grundläggande för att motverka risken för att verksamheten utnyttjas. Finansinspektionen anför därför att det finns skäl att se strängt på överträdelserna. Loomis tilldelas därför en anmärkning och åläggs att betala en sanktionsavgift om 40 miljoner kronor.

4 Wesslau Söderqvist Advokatbyrås rekommendationer

Finansinspektionens beslut signalerar tydligt vikten vid att verksamhetsutövares arbete med att förhindra penningtvätt och finansiering av terrorism består av flera samverkande åtgärder. Detta då en brist i någon del av arbetet riskerar att orsaka brister även i andra rutiner och processer.

Wesslau Söderqvist Advokatbyrå rekommenderar mot bakgrund av Finansinspektionens beslut att kreditgivare och även andra finansiella företag löpande genomför riskbedömningar för att identifiera och hantera potentiella risker. Därutöver är det viktigt att göra riskbedömningar av kunder och individualiserade bedömningar av om kunderna driver kontantintensiv verksamhet, liksom att vidta ytterligare åtgärder för kundkännedom. Detta gäller alla verksamheter, men särskilt långtgående krav ställs på kontantintensiva verksamheter att vidta åtgärder för att förhindra att de kan utnyttjas för kriminella syften. Riskbedömning av verksamheten och kunder måste ske på löpande basis och högre krav ställs i de delar riskerna bedöms som höga.

Har ni frågor med anledning av det ovanstående, eller önskar vägledning avseende allmänna riskbedömningar, hantering av högriskkunder eller andra kundkännedomsåtgärder, är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå.

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. Vägledning för upprättande av PRIIP-faktablad för fonder

---

5 juli 2024

1 Bakgrund

Fondbolagens förening har tagit fram vägledning för att underlätta upprättande och översyn av PRIIP-faktablad för fonder. Vägledningen syftar dels till att hjälpa fondbolag genom att sammanställa gällande regelverk, dels till att hjälpa fondbolag att tolka regelverken.

Enligt PRIIP-förordningen[1] ska faktablad tas fram för paketerade försäkringsbaserade investeringsprodukter för icke-professionella investerare, s.k. PRIIP-produkter. Ursprungligen har fonder medgivits ett undantag från att producera PRIIP-faktablad då fonder tillhandahåller fondfaktablad. Från den 1 januari 2023 ställs det dock krav på att fonderna ska upprätta PRIIP-faktablad. För att säkerställa att icke-professionella investerare inte får två olika faktablad och att företag inte ska behöva tillhandahålla två faktablad för samma finansiella produkt fastställer 4 kap. 16 b § lagen (2004:46) om värdepappersfonder att faktablad uppfyller kraven om det upprättas, tillhandahålls, ändras och översätts enligt kraven i PRIIP-förordningen.

Nedan följer en kort redogörelse för vägledningens innehåll med fokus på den vägledning som Fondbolagens förening tagit fram avseende PRIIP-faktabladen.

2 Allmänt om PRIIP-faktabladet

2.1 Upprättande och tillhandahållande av faktabladet

PRIIP-produktutvecklaren ska utforma ett faktablad och göra det tillgängligt på sin webbplats innan produkten görs tillgänglig för icke-professionella investerare. Den som ger råd om eller säljer produkten ska kostnadsfritt förse investeraren med faktabladet i god tid innan avtalet eller erbjudandet blir bindande.

2.2 Översyn/revideringar av faktabladet

En översyn av informationen bör göras när det sker en förändring som har eller sannolikt kommer att få avsevärd inverkan på informationen, eller åtminstone var tolfte månad efter

[1] *Europaparlamentets och rådets förordning (EU) nr 1286/2014 av den 26 november 2014 om faktablad för paketerade och försäkringsbaserade investeringsprodukter för icke-professionella investerare (PRIIP-produkter).*

första offentliggörandet. Om förändringen innebär att det blir aktuellt att göra ändringar av faktabladet ska ändringarna publiceras utan onödigt dröjsmål.

2.3 Marknadsföringsmaterial

Faktabladet ska vara ett fristående dokument, skiljt från marknadsföringsmaterial, och får inte innehålla hänvisningar till marknadsföringsmaterial. Därtill får inte marknadsföringsmaterialet innehållande särskilda uppgifter om PRIIP-produkten bestå av uppgifter som strider mot informationen i faktabladet eller information som minskar dess betydelse. Däremot ska marknadsföringsmaterialet innehålla uppgifter om faktabladets existens och om hur och varifrån det kan erhållas.

3 PRIIP-faktabladets innehåll och utformning

Nedan följer en kort sammanfattning av vägledningen som Fondbolagens förening har tagit fram utifrån kraven i PRIIP-förordningen.

- Faktabladets mall och form: PRIIP-produktutvecklaren ska upprätta ett faktablad utifrån den mall som finns i bilaga I till PRIIP-förordningen. Mer specifikt ska faktabladet vara kort och koncist och högst tre A4-sidor långt, med särskilt fokus på de basfakta som icke-professionella investerare har behov av att ta del av. Språket ska vara klart, koncist och begripligt och faktabladet ska tillhandahållas på ett av distributionslandets officiella språk, eller på ett annat språk som godtas av behörig myndighet i landet.

- Allmän information: Avsnittet med allmän information ska benämnas med rubriken ”Produkt”. Därutöver ska fondens namn och ISIN-nummer anges samt den andelsklass som faktabladet avser samt om fonden har flera andelsklasser. Vidare ska uppgift om fondbolagets namn, telefonnummer, webbsida och tillsynsmyndighet lämnas. Om fondbolaget är auktoriserat ska koncernens namn anges. I tillämpliga fall ska också en varningstext finnas med, se närmare i artikel 8.3b och 25.4 i PRIIP-förordningen.

- ”Vad innebär produkten?”: I avsnittet ska anges vilken typ av produkt som fonden avser och dess juridiska form, dvs. om det är en värdepappersfond eller en specialfond. Vidare ska fondens ”syften och hur de ska uppnås” specificeras. Därtill ska vilka faktorer som ska bestämma avkastningen anges, underliggande tillgångar eller referensvärden och hur avkastningen fastställs. PRIIP-dokumentet ska därutöver innehålla information om den tänkta investerare som PRIIP-tillverkaren identifierat som målgrupp.

- **Risker/avkastning:** En kortfattad beskrivning av PRIIP-produktens risk- och avkastningsprofil ska inkluderas vilket innefattar en bedömning av marknadsrisken, kreditrisken för underliggande tillgångar samt en kreditriskbedömning. Informationen ska ses över när en ändring som har avsevärd inverkan på informationen sker och åtminstone var tolfte månad efter första publicering. I vägledningen återfinns exempel på hur den sammanfattande riskindikatorn kan presenteras, se närmare i avsnitt 1.4 i vägledningen.

- **Resultatscenarier:** Fyra resultatscenarier ska visas, bestående av ett positivt, ett neutralt, ett negativt och ett stresscenario. Därtill ska ett minimumscenario visas. Resultatet ska beräknas efter avdrag för alla relevanta kostnader för presenterad innehavsperiod vilket betyder att exempelvis avgifter för korttidshandel bara ska tas med om de är relevanta i förhållande till ifrågavarande period. Avkastningen ska beräknas på insatt belopp, presenteras i monetära termer, avrundas och presenteras i procent som årlig genomsnittlig avkastning. I avsnitt 1.5 i vägledningen preciseras metoden för presentationen samt hur och när översyn ska göras.

- **”Vad händer om [namnet på PRIIP-produktutvecklaren] inte kan göra några utbetalningar?”:** I detta avsnitt ska fondbolaget beskriva vad som händer om bolaget inte kan göra några utbetalningar eller inte kan uppfylla sina åtaganden. Fondbolaget ska därtill förklara förvaringsinstitutets funktion samt ange om förlusten täcks av en kompensationsordning eller garantiordning.

- **”Vilka är kostnaderna?”:** I bilaga VI till PRIIP-förordningen återfinns en metod för beräkning av kostnaderna. I korthet ska listan över kostnader redovisas där transaktionskostnader ska ingå, till skillnad från kostnader för UCITS-faktablad. I avsnitt 1.7 i vägledningen beskrivs närmare hur beräkningen ska gå till, vilka krav som ställs samt hur kostnaderna ska presenteras och sammansättas.

- **”Hur länge bör jag behålla investeringsprodukten och kan jag ta ut pengar i förtid?”:** I avsnittet ska anges och motiveras hur länge investeraren bör behålla fonden. Därtill ska en beskrivning av förfarandet för att avveckla investeringen anges inklusive hur förtida inlösen påverkar fondens risk- eller resultatprofil samt om det kan innebära avgifter om fonden säljs inom en viss tid.

- **”Hur kan jag klaga”:** Avsnittet ska innehålla information om var investeraren kan vända sig med eventuella klagomål och en länk till fondbolagets webbplats samt postadress och e-postadress. Se närmare i avsnitt 1.9 i vägledningen.

- **”Övrig relevant information”:** I avsnittet ska fonden upplysa om var andra informationsdokument finns att tillgå, lämpligen med en länk till fondbolagets hemsida. Därtill ska information redovisas om det antal år som avkastningsdata visar och information om historiska resultatscenarier, offentliggjorda på månadsbasis.

- **Översyn och ändring av faktabladet:** Slutligen ska faktabladet ses över när en ändring med avsevärd inverkan på informationen sker, eller åtminstone var tolfte månad. Processer ska finnas som medför att fondbolaget utan onödigt dröjsmål kan upptäcka omständigheter som kan leda till förändringar. Utan onödigt dröjsmål ska faktabladet ändras när så är nödvändigt, vilket ska offentliggöras på fondbolagets webbplats.

Observera att vägledningen som Fondbolagens förening presenterar innefattar mallar och närmare anvisningar avseende faktabladen. I vägledningen presenteras ytterligare information om särskilda bestämmelser för faktabladen för PRIIP-produkter som erbjuder flera olika investeringsalternativ och också information om fond som underliggande investeringsalternativ.

4 Wesslau Söderqvist Advokatbyrås rekommendationer

För att säkerställa en effektiv implementering och översyn av PRIIP-faktabladet rekommenderas att fondbolag tar del av den fullständiga vägledningen från Fondbolagens förening, inklusive de mallar och detaljerade anvisningar som återfinns i vägledningen. Genom att följa vägledningen kan fondbolag säkerställa att deras PRIIP-faktablad uppfyller de krav som ställs och tillhandahålla tydlig och begriplig information för icke-professionella investerare.

Wesslau Söderqvist Advokatbyrå rekommenderar att samtliga fondbolag ska se över sina faktablad och att ändringar ska göras i befintliga faktablad i de fall den reviderade vägledningen resulterar i att ändringar behöver göras för att efterleva PRIIP-förordningen. Advokatbyrån är behjälplig med att genomföra de ändringar och krav som specificeras i vägledningen eller att se över de faktablad som upprättas. Har ni frågor med anledning av det ovanstående är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå.

Nyhetsbrev

Ang. Granskning av dataskyddsombudens roll och ställning

---

9 juli 2024

1 Bakgrund

Den Europeiska dataskyddstyrelsen tillsammans med de nationella dataskyddsmyndigheterna, däribland Integritetsskyddsmyndigheten, inledde år 2023 en samordnad åtgärd med syftet att undersöka dataskyddsombudets roll och ställning. Integritetsskyddsmyndigheten har som del i arbetet inlett tillsyn mot ett 50-tal organisationer som samtliga har dataskyddsombud, och en fördjupad granskning avseende sex av verksamheterna.

Enligt dataskyddsförordningen, nedan GDPR, är vissa verksamheter skyldiga att utse dataskyddsombud vars uppgift är att bidra till att den egna verksamheten följer dataskyddslagstiftningen. Ett ombud får därutöver utföra andra uppgifter och uppdrag, förutsatt att det inte leder till intressekonflikter. I enlighet med GDPR måste ombudens oberoende och förmåga att effektivt utföra sina dataskyddsuppgifter säkerställas.

Förra veckan publicerades Integritetskyddsmyndighetens fördjupade granskning som avslutar arbetet med Dataskyddsstyrelsens samordnade åtgärd. Integritetskyddsmyndighetens arbete att vägleda dataskyddsombud fortsätter emellertid i andra former, bland annat har två referensgrupper upprättats för att föra en kontinuerlig dialog och fånga upp behov av ny vägledning för dataskyddsombuden. Nedan följer en kort översikt avseende de iakttagelser som Dataskyddsstyrelsen och Integritetsskyddsmyndigheten har identifierat.

2 Närmare om den Euroepiska dataskyddsstyrelens granskning

2.1 Undersökningen

I januari år 2024 publicerade Dataskyddsstyrelsen en rapport som sammanställde nationella iakttagelser av om dataskyddsombuden har den roll och ställning som krävs enligt artiklarna 37 – 39 i GDPR, samt om de har de resurser som de behöver för att utföra sina uppgifter. Olika organisationer och dataskyddsombud kontaktades utifrån ett brett spektrum av sektorer, både inom offentlig och privat sektor. Rapporten listar hinder som skyddsombuden står inför, tillsammans med rekommendationer för att ytterligare stärka skyddsombudens roll.

2.2 Undersökningens resultat

Trots vissa farhågor och utmaningar som dataskyddsombud står inför är resultaten av granskningen huvudsakligen uppmuntrande. Dataskyddsstyrelsen uppmärksammar att majoriteten av dataskyddsombuden har de färdigheter och kunskaper som krävs för att utföra arbetet och att de regelbundet får utbildning i dataskyddsfrågor. Därtill har de väl definierade uppgifter och utsätts sällan för påtryckningar om hur arbetet ska utföras.

De utmaningar som identifieras är att utse uppgiftsskyddsombud trots att det är obligatoriskt, otillräckliga resurser eller expertkunskaper samt att dataskyddsombuden inte fullt ut anförtros de uppgifter som föreskrivs i GDPR. Mot bakgrund av utmaningarna ger rapporten vissa rekommendationer till organisationer, dataskyddsombud och dataskyddsmyndigheter. Dataskyddsmyndigheter uppmuntras att genomföra medvetandehöjande åtgärder samt informations- och tillsynsåtgärder. Därtill betonas vikten vid att organisationer säkerställer att skyddsombud har tillräckliga möjligheter, tid och resurser för att kontinuerligt uppdatera sin kunskap och lära sig om den senaste utvecklingen på området.

3 Närmare om Integritetsskyddsmyndighetens granskning

3.1 Undersökningen

I Integritetskyddsmyndighetens tillsyn har organisationer besvarat frågor avseende dataskyddsombudens kvalifikationer, uppgifter och ställning med syftet att bedöma om deras roll och ställning svarar mot kraven i GDPR och om de har de resurser som behövs för att utföra sina uppgifter effektivt. En fördjupad granskning inleddes därefter med ett mindre urval verksamheter och kretsade kring några särskilt viktiga frågeställningar.

De verksamheter som ingått i den fördjupade tillsynen är Hemköpskedjan AB, PostNord Sverige AB, Regionstyrelsen i Region Västerbotten, Socialnämnden i Stockholms stad, Socialnämnden i Örebro kommun och Swedavia AB. Gemensamt för verksamheterna är att dataskyddsombuden har haft andra uppdrag utöver att bidra till att den egna verksamheten följer dataskyddslagstiftningen. Bland annat har dataskyddsombuden haft uppdrag som informationssäkerhetschefer, haft specifika ansvarsområden inom compliance, risk och säkerhet, och arbetat som förvaltningsjurister eller regionsjurister.

3.2 Undersökningens resultat

I besluten poängteras att funktioner som innebär ledande befattningar typiskt sett kan ge upphov till intressekonflikt med rollen som dataskyddsombud, i strid med GDPR. Detta eftersom det ofta innebär att ombudet är delaktigt i beslut rörande personuppgiftsbehandlingar på ett sådant sätt att skyddsombudets oberoende kan ifrågasättas. PostNords dataskyddsombud som innehar ledaransvar inom områdena compliance, risk och säkerhet, Hemköps dataskyddsombud som är Risk Manager, Socialnämnden i Stockholms dataskyddsombud som arbetar som förvaltningsjurist och Swedavias dataskyddsombud som arbetar som informationssäkerhetschef bedöms mot den bakgrunden inte medföras ansvar som leder till delaktighet i beslut som gäller ändamål och medel för personuppgiftsbehandlingar.

I sin tillsyn har Integritetsskyddsmyndigheten däremot identifierat brister i Region Västerbottens verksamhet, i vilken skyddsombudet också är regionsjurist vid ledningsstaben. Dataskyddsombudet ska oberoende och självständigt granska organisationens efterlevnad av dataskyddslagstiftningen, vilket omfattar granskning av dataskyddsarbetet i ledningsstaben. Eftersom regionsjuristen är delaktig i ledningsstaben genom rådgivning bedömer Integritetsskyddsmyndigheten att det funnits en intressekonflikt i strid med reglerna i GDPR.

Ytterligare en brist har identifierats hos Socialnämnden i Örebro eftersom varsamheten inte på ett korrekt sätt eller i god tid säkerställt att skyddsombudet deltagit i alla frågor som rör personuppgiftsskyddet. Integritetskyddsmyndigheten bedömer även att verksamheten inte stöttat ombudet tillräckligt genom att tillhandahålla de resurser som krävs och inte heller säkerställt att ombudet rapporterat direkt till socialnämndens högsta förvaltningsnivå. Med anledning av bristerna tilldelas Region Västerbotten och Socialnämnden i Örebro reprimander.

4 Wesslau Söderqvist Advokatbyrås rekommendationer

För att säkerställa effektiv efterlevnad av GDPR och ett tillfredsställande säkerhetsarbete genom dataskyddsombud rekommenderas att verksamheter tar del av de fullständiga rapporter som den Europeiska dataskyddsstyrelsen och Integritetsskyddsmyndigheten publicerat.

Wesslau Söderqvist Advokatbyrå rekommenderar ett kontinuerligt arbete för att stärka dataskyddsombudens roll och ställning. Särskilt viktigt är det, för de verksamheter som enligt GDPR är skyldiga att utse dataskyddsombud, att skyddsombudets oberoende och självständighet garanteras, och att skyddsombud erhåller de möjligheter, den tid och de resurser som krävs för att kunna utföra ett effektivt arbete. Därutöver måste säkerställas att skyddsombuden har de färdigheter och kunskaper som krävs och att de regelbundet och

kontinuerligt får uppdatera sina kunskaper och lära sig om den senaste utvecklingen på området.

Har ni frågor avseende de krav som ställs enligt GDPR eller eventuella intressekonflikter kopplade till dataskyddsombuden får ni gärna kontakta Wesslau Söderqvist Advokatbyrå.

Nyhetsbrev

Ang. teknisk standard om incidenthantering

---

11 juli 2024

1 Sammanfattning av delegerad förordning (EU) 2024/1772

1.1 Syfte och mål

Europeiska kommissionen har antagit en förordning som syftar till att specificera klassificeringskriterier och väsentlighetströsklar för att fastställa och rapportera allvarliga incidenter och betydande cyberhot inom finanssektorn. Förordningen kompletterar Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (DORA). Förordningen har som mål att harmonisera rapporteringskraven för IKT-relaterade incidenter, informations- och kommunikationsteknologi och andra operativa eller säkerhetsrelaterade incidenter som påverkar kreditinstitut, betalningsinstitut, leverantörer av kontoinformationstjänster och institut för elektroniska pengar. Med beaktande av proportionalitetsprincipen bör klassificeringskriterierna och väsentlighetströsklarna återspegla storleken och den övergripande riskprofilen samt karaktären, omfattningen och komplexiteten hos alla finansiella enheters tjänster. Målet är att skapa en konsekvent och proportionell metod för incidentrapportering som inte belastar mindre finansiella enheter på ett oproportionerligt sätt.

Denna förordning ska tillämpas från och med den 17 januari 2025.

1.2 Klassificeringskriterier

Förordningen anger kriterier för att klassificera incidenter som allvarliga. Dessa inkluderar följande:

1. Antal kunder och finansiella motparter som påverkas av incidenten. Antalet berörda kunder och finansiella motparter samt incidentens inverkan på affärsmål och marknadseffektivitet. Den finansiella enheten ska beakta hur påverkan på en kund eller en finansiell motpart kan inverka på uppfyllandet av enhetens verksamhetsmål samt incidentens möjliga inverkan på marknadseffektiviteten.

2. Påverkan på finansiella enheters anseende, det räcker med att ett av följande kriterier är uppfyllt. Incidentens synlighet i media, kundklagomål, förutsättningen att uppfylla lagstadgade krav till följd av incidenten och potentiell kundförlust. När finansiella enheter bedömer incidentens påverkan på anseendet ska de beakta hur mycket uppmärksamhet incidenten har fått eller sannolikt kommer att få i förhållande till varje angivet kriterium.

3. Varaktighet och tjänstavbrott. Hur länge incidenten pågår samt hur tjänstens tillgänglighet påverkas. Finansiella enheter ska mäta incidentens varaktighet från den tidpunkt den inträffar fram tills att den är löst. Om detta inte är möjligt, ska de mäta varaktigheten från när den upptäcktes, alternativt utföra skattningar.

4. Geografisk spridning. Incidentens påverkan på flera medlemsstater och betydelsen av effekterna i andra jurisdiktioner. Effekten ska baseras på kunder och finansiella motparter i andra medlemsstater, filialer eller andra finansiella enheter inom koncernen som verkar i andra medlemsstater, alternativt finansmarknadsinfrastrukturer eller tredjepartsleverantörer som kan påverka finansiella enheter i andra medlemsstater till vilka de tillhandahåller tjänster i den mån sådan information är tillgänglig.

5. Dataförluster. Finansiella enheter ska ta hänsyn till huruvida uppgifters tillgänglighet, äkthet, integritet och konfidentialitet påverkas.

6. Tjänsternas allvarlighetsgrad. Om incidenten påverkar kritiska eller viktiga funktioner eller finansiella tjänster.

7. Ekonomiska konsekvenser. Direkta eller indirekta kostnader och förluster som inträffar till följd av incidenten, inklusive stulna tillgångar, personalkostnader, avgifter på grund av att avtalsförpliktelser inte har fullgjorts, kostnader för gottgörelse och ersättning till kunder, förluster på grund av uteblivna intäkter, rådgivningskostnader, inklusive kostnader i samband med juridisk rådgivning, kriminaltekniska tjänster och saneringstjänster.

1.3 Allvarliga incidenter och väsentlighetströsklar

Förordningen specificerar väsentlighetströsklar som ska användas för att avgöra om en incident är allvarlig nog för att rapporteras:

- Trösklarna är avsedda att vara proportionella mot finansiella enheters storlek, riskprofil och komplexitet.

- Incidents ekonomiska konsekvenser och dess inverkan på verksamheten och kunder i andra medlemsstater är centrala i bedömningen.

- Återkommande incidenter med liknande grundorsaker kan betraktas som allvarliga om de tyder på brister i enhetens riskhanteringsförfaranden.

- Kriteriet för väsentlighet är uppfyllt för kunder, finansiella motparter och transaktioner om något av följande villkor är uppfyllda:

    1. Antalet påverkade kunder överstiger 10 % av alla kunder som använder den aktuella tjänsten,

    2. antalet påverkade kunder som använder den aktuella tjänsten överstiger 100 000,

    3. antalet påverkade finansiella motparter överstiger 30 % av alla finansiella motparter som är involverade i tillhandahållandet av den aktuella tjänsten,

    4. antalet påverkade transaktioner överstiger 10 % av det dagliga genomsnittet av transaktioner utförda av den finansiella entiteten i samband med den aktuella tjänsten och

    5. värdet av de påverkade transaktionerna överstiger 10 % av det dagliga genomsnittliga transaktionsvärdet som utförs av den finansiella entiteten i samband med den aktuella tjänsten, eller att kunder eller finansiella motparter har identifierats som relevanta.

- Om det faktiska antalet kunder eller finansiella motparter som påverkas eller det faktiska antalet eller den faktiska mängden transaktioner som påverkas inte kan fastställas, ska den finansiella entiteten uppskatta dessa på grundval av tillgängliga uppgifter från jämförbara referensperioder.

1.4 Användning och rapportering

För att säkerställa att incidentrapporter används effektivt för tillsyn och för att förhindra spridningseffekter inom finanssektorn, ska rapporterna omfatta detaljerade uppgifter om incidentens påverkan och de åtgärder som vidtagits. Incidenter som utgör personuppgiftsincidenter enligt GDPR ska rapporteras i enlighet med GDPR. Det innebär att finanssektorns aktörer måste följa GDPR-krav när personuppgifter är involverade i incidenten.

Sammanfattningsvis syftar förordningen till att förbättra den digitala operativa motståndskraften i EU-finanssektor genom att skapa en enhetlig och rättvis metod för rapportering av IKT-relaterade incidenter och cyberhot.

2 Wesslau Söderqvist Advokatbyrås rekommendationer

2.1 Implementera ett incidenthanteringssystem

Det är av betydelse att införliva en incidentidentifiering och klassificering genom att säkerställa att det finnsmekanismer för att snabbt identifiera, klassificera och spåra IKT-relaterade incidenter. Wesslau Söderqvist Advokatbyrå rekommenderar en översyn av de rutiner och processer som krävs för att rapportera allvarliga incidenter till Finansinspektionen. Om en incident inträffar rekommenderas att dokumentera och övervaka antalet kunder och finansiella motparter som påverkas. Det är även av betydelse att bevaka incidentens påverkan på verksamhetens anseende, mäta och registrera varaktigheten samt driftstoppet för incidenten. Wesslau Söderqvist Advokatbyrå rekommenderar även att incidentens geografiska påverkan och dataförluster bedöms och dokumenteras vid en incident. Det är även av vikt att identifiera och kategorisera kritiska tjänster, bedöma incidentens påverkan på dessa och beräkna de ekonomiska konsekvenserna av incidenter.

2.2 Utveckla och implementera kontinuitets- och beredskapsplaner

Wesslau Söderqvist Advokatbyrå rekommenderar att befintliga beredskaps- och kontinuitetsplaner som hanterar potentiella IKT-relaterade incidenter och cyberhot ses över och kompletteras enligt DORA. Det är även av betydelse att säkerställa att tredjepartsleverantörer som påverkar verksamheten omfattas av kontinuitetsplaner och incidentrapportering. Detta kan kräva översyn av befintliga IKT-avtal.

2.3 Analysera och förbättra incidenthantering efter varje incident

Efter varje incident rekommenderar vi er att genomföra en detaljerad analys samt granska bolagets återkoppling och hantering. Det är även av relevans att identifiera och implementera förbättringar som är baserade på lärdomar från tidigare incidenter för att kunna stärka framtida hantering. Genom att följa dessa rekommendationer förstärks säkerställandet av efterlevnad av den delegerade förordningen och den operativa motståndskraften, samt minimeras riskerna för allvarliga incidenter.

Har ni frågor avseende de krav som ställs enligt ovan gällande incidenthantering eller om DORA generellt får ni gärna kontakta Wesslau Söderqvist Advokatbyrå.

Nyhetsbrev

Ang. kontraktsmässiga arrangemang

---

11 juli 2024

1 Sammanfattning av delegerad förordning (EU) 2024/1773

1.1 Bakgrund och syfte

Europeiska kommissionen har nyligen antagit en förordning som kompletterar Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (DORA). Den kompletterande förordningen rör kontraktsrättsliga arrangemang och hanteringen av IKT-tredjepartsrisker. Förordningen påverkar inte skyldigheter enligt GDPR och inte heller kravet på att ha skriftliga personuppgiftsbiträdesavtal. Förordningen syftar till att säkerställa transparent och ansvarsfull hantering av leverantörsrelationer för att upprätthålla integritet och effektivitet i den finansiella verksamheten.

Denna förordning ska tillämpas från och med den 17 januari 2025.

1.2 Hantering av IKT-tredjepartsrisker

Finansiella enheter ska etablera och regelbundet revidera strategier för hantering av risker kopplade till tredjepartsleverantörer av IKT-tjänster. Strategin ska omfatta policyer för kritiska eller viktiga funktioner som stöds av dessa leverantörer och tillämpas både på individuell och gruppnivå. Förordningen tar hänsyn till variationen i storlek, struktur och komplexitet bland finansiella enheter. Kraven ska tillämpas på ett sätt som är proportionellt med ovanstående skillnader. Ledningen bär det yttersta ansvaret för att hantera IKT-risker, inklusive risker som uppstår vid användning av tredjepartsleverantörer. De måste säkerställa att policyn antas och revideras minst en gång per år. Policyn ska innehålla detaljer om planering, genomförande, övervakning och förvaltning av kontraktsmässiga arrangemang med tredjepartsleverantörer, inklusive exitstrategier och avslutningsförfaranden.

1.3 Grupp-program och styrformer

Vid tillämpning av denna förordning på undergrupps- eller gruppnivå åligger det moderföretaget som har ansvaret för att tillhandahålla koncernredovisningen eller

undergruppsredovisningen att säkerställa en enhetlig tillämpning av policyn i samtliga finansiella enheter som ingår i koncernen. Ledningsorganet bär ansvar att se över policyn minst en gång om året och uppdatera den vid eventuella behov. Ändringar i policyn ska utgöras i god tid och så snart det är möjligt inom ramen för de relevanta avtalsarrangemangen. Den finansiella enheten ska dokumentera den planerade tidsplanen för genomförandet. Policyn syftar till att etablera tydliga riktlinjer för hantering av IKT-tjänster som understödjer kritiska eller viktiga funktioner inom finansiella enheter. För det första fastställs eller refereras en metod för att identifiera sådana tjänster samt hur och när bedömningen av dem ska utföras och granskas. Ansvarsfördelningen internt identifieras tydligt för godkännande, ledning, kontroll och dokumentation av relevanta kontraktsmässiga arrangemang. Det försäkras att nödvändiga färdigheter och kunskaper upprätthålls för effektiv övervakning av dessa arrangemang, inklusive de IKT-tjänster som omfattas.

1.4 Policy

Intern policy kräver även att tredjepartsleverantörer av IKT-tjänster ska bedömas för att säkerställa att de har tillräckliga resurser för att möta alla juridiska och regulatoriska krav som den finansiella enheten är skyldig att uppfylla. Policyn ska säkerställa att finansiella enheter har rätt att få tillgång till information, genomföra inspektioner, revisioner och IKT-tester enligt fastställda metoder, inklusive intern revision eller tredjepartsrevisioner. En specifik roll inom den verkställande ledningen tillskrivs ansvaret för övervakningen av dessa kontraktsarrangemang, med tydliga riktlinjer för samarbete med kontrollfunktioner och rapporteringsvägar till ledningsorganet. Kontraktsmässiga arrangemang ska vara förenliga med en rad specifika ramar och planer för IKT-riskhantering, informationssäkerhet, IKT-kontinuitet och incidentrapportering enligt relevanta EU-förordningar. Policyn inkluderar krav på oberoende granskning av IKT-tjänster som stödjer kritiska funktioner och deras inkludering i revisionsplaner.

Policyn ska specificera övervakning av kontraktsmässiga arrangemang, inklusive åtgärder vid avtalsbrott och en dokumenterad plan för avtalsuppsägning. Kontraktsmässiga arrangemang befriar inte den finansiella enheten från lagstadgade skyldigheter gentemot kunder. Den finansiella enheten får inte förhindra effektiv tillsyn eller överträda tillsynsrestriktioner. Den finansiella enheten ska säkerställa samarbete med behöriga myndigheter, tillhandahålla tillgång till relevant data och lokaler för revison och tillsyn av IKT-tjänster som stödjer kritiska eller andra viktiga funktioner.

1.5 Riskbedömning

Policyn föreskriver också att en omfattande riskbedömning ska genomföras på flera nivåer för finansiella enheter samt på gruppnivå och undergruppsnivå vid behov innan avtal ingås. Riskbedömningen måste ta hänsyn till alla relevanta krav och tillämplig sektorsspecifik unionslagstiftning. Särskilt viktigt är att bedöma hur tredjepartsleverantörer av IKT-tjänster levererar stödjande tjänster för kritiska eller viktiga funktioner inom den finansiella enheten samt identifiera risker i samband med dessa tjänster.

Det innefattar operativa, rättsliga, IKT-relaterade, renommé-, och konfidentialitets- och personlighetsuppgiftskydds-, datatillgångs-, datahanteringsplats-, leverantörsplats- samt IKT-koncentrationsrisker på entitetsnivå. Åtgärderna syftar till att säkerställa att den finansiella enheten, innan avtal ingås, innehar en grundläggande kunskap för sina affärsbehov, bedömer och hanterar de mångfacetterade riskerna som är förknippade med tredjepartsleverantörers IKT-tjänster som stödjer dess kritiska funktioner.

1.6 Tillbörlig aktsamhet

Den föreslagna policyn syftar till att etablera tydliga och proportionella riktlinjer för att välja och bedöma leverantörer av IKT-tjänster för finansiella enheter. Syftet är att säkerställa att leverantören uppfyller standarderna angående kapacitet, kompetens, resurser och säkerhetsåtgärder som är nödvändiga för att stödja kritiska eller viktiga funktioner. Policyn ställer krav på att finansiella enheter genomför en noggrann bedömning av potentiella leverantörer innan avtal ingås. Bedömningen baseras på leverantörens affärsrykte, kapacitet, tekniska kunskaper, resurser såsom ekonomiska och personella resurser, samt deras förmåga att upprätthålla höga standarder inom informationssäkerhet, riskhantering och interna kontroller. Leverantören ansvarar också för att följa och tillämpa ledande praxis inom IKT-säkerhet och att inneha förmåga att hantera och överväga teknisk utveckling.

Leverantören ska godkänna kontraktsmässiga revisioner för att möjliggöra granskningar från den finansiella enheten eller auktoriserade myndigheter. Policyn specificerar även säkerhetsnivån som krävs för IKT-tjänsternas riskhanteringsram, inklusive krav på riskreducerande och kontinuitetsåtgärder. Metoder för att bedöma leverantörens prestation inkluderar revisioner, oberoende bedömningar,

revisionsrapporter och certifieringar från tredje part samt annan relevant tillgänglig information.

1.7 Rapportering och övervakning

Policyn ska fastställa interna ansvarsområden för godkännande och övervakning av avtal med tredjepartsleverantörer. Den ska även säkerställa att lämplig rapportering till ledningsorganet sker regelbundet. Policyn kräver att finansiella enheter identifierar, förebygger och hanterar intressekonflikter som kan uppstå med tredjepartsleverantörer av IKT-tjänster innan avtal ingås. Det krävs även kontinuerlig övervakning av sådana konflikter. Om koncerninterna IKT-tjänster används för kritiska funktioner måste policyn säkerställa objektiva beslut om avtalsvillkor, inklusive ekonomiska aspekter.

2 Wesslau Söderqvist Advokatbyrås rekommendationer

Wesslau Söderqvist Advokatbyrå rekommenderar att det antas och införlivas en policy som anpassas efter den specifika enhetens storlek, övergripande riskprofil samt arten och omfattningen av de tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster i enlighet med vad som framgår av den kompletterande förordningen.

En central del av policyn bör vara en noggrann riskbedömning på både enskild enhetsnivå och eventuellt på gruppnivå. Det är viktigt att identifiera och bedöma alla operativa, rättsliga och IKT-relaterade risker som är förknippade med användningen av tredjepartsleverantörer av IKT-tjänster. Denna bedömning bör även omfatta faktorer som leverantörens rykte, tekniska kapacitet, säkerhetsstandarder och förmåga att hantera krav på konfidentialitet och dataskydd.

Policyn bör tydligt fastställa ansvarsområden och metoder för godkännande, ledning och övervakning av de kontraktsmässiga arrangemangen. Det är viktigt att en dedikerad funktion eller medlem av den verkställande ledningen utses för att säkerställa att övervakningen av tredjepartsleverantörernas prestationer sker regelbundet och effektivt. Rapporteringsvägarna till ledningsorganet bör också specificeras för att säkerställa en snabb hantering av eventuella incidenter eller problem.

Har ni frågor med anledning av det ovanstående är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå. Vi har god erfarenhet av att se över och anpassa IKT-avtal i enlighet med DORA och bistår er gärna.

Nyhetsbrev

Ang. IKT-säkerhet och IKT-risker

---

11 juli 2024

1 Sammanfattning av delegerad förordning (EU) 2024/1774

1.1 IKT-säkerhet och riskhantering

Europeiska kommissionen har antagit en förordning som reglerar hantering av IKT-säkerhet och IKT-risker inom finansiella enheter och omfattar flera aspekter från övergripande riskprofiler till specifika procedurer för sårbarhetshantering. Förordningen kompletterar Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (DORA). Finansiella enheter ska vid utarbetande och genomförande av riktlinjer och verktyg för IKT-säkerhet beakta enhetens storlek, riskprofil och tjänsternas komplexitet. Detta inkluderar kryptering, nätverkssäkerhet, förändringsledning och påverkan på dataintegritet och tillgänglighet.

Denna förordning ska tillämpas från och med den 17 januari 2025.

1.2 IKT-säkerhetspolicyer och verktyg

Finansiella enheter ska utveckla strategier och protokoll som inkluderar nätverkssäkerhet, skydd mot dataintrång och bibehållande av dataintegritet och konfidentialitet. Dessa ska vara anpassade till enhetens informationssäkerhetsmål och strategier för digital operativ motståndskraft. Enheterna ska dokumentera och genomföra riktlinjer för att hantera IKT-risker inklusive identifiering av sårbarheter, riskbedömning och implementering av krishanteringsåtgärder. Årliga översyner av kvarstående risker är obligatoriska.

1.3 Förvaltning av IKT-tillgångar

Finansiella enheter ska ha en policy för livscykelhantering av IKT-tillgångar som inkluderar övervakning, dokumentation och klassificering. Kritiska tillgångar ska dokumenteras noggrant med information om ägare, placering och beroenden. Policyn ska inkludera kryptering av data i vila och under överföring, hantering av krypteringsnycklar samt krav på att uppdatera krypteringstekniker för att säkerställa motståndskraft mot cyberhot.

1.4 Säkerhet i IKT-verksamheten

Finansiella enheter ska utarbeta riktlinjer för säker installation, underhåll och återställning av IKT-system. Detta inkluderar säkerhetskopiering, övervakning och hantering av fel samt åtskillnad mellan produktions- och testmiljöer. Förfaranden ska säkerställa identifiering av kapacitetskrav och optimera resursanvändning för att upprätthålla och förbättra systemens tillgänglighet och effektivitet. Förfaranden ska identifiera och hantera sårbarheter genom regelbundna analyser och uppdateringar. Tredjepartsleverantörer ska övervakas för att säkerställa att de hanterar sårbarheter i tillhandahållna tjänster.

1.5 Data- och systemsäkerhet

Finansiella enheter ska skapa och implementera omfattande säkerhetsförfaranden för data och IKT-system. Det ska inkludera åtgärder som åtkomstbegränsningar, säker konfigurationsbaslinje och åtgärder mot skadlig kod och otillåten programvara. Säkerhetsåtgärder ska säkerställa att endast godkända datalagringsmedier och system används. Det inkluderar krav på hantering av portabla och privata slutpunktsenheter, säker radering av data och avveckling av datalagringsenheter som innehåller konfidentiell information.

1.6 Loggning och händelsespårning

Finansiella enheter ska utveckla loggnigsprocedurer för att identifiera och logga relevanta händelser, säkerställa att loggar skyddas mot manipulation och för att upptäcka systemfel. Loggarna ska kunna användas för att effektivt upptäcka onormal verksamhet.

1.7 Hantering av nätverkssäkerhet

Finansiella enheter ska genomföra åtgärder för att skydda sina nätverk mot intrång och dataförlust. Detta inkluderar segmentering av nätverk, dokumentation av nätverksanslutningar, användning av dedikerade nätverk för hantering av IKT-tillgångar och kryptering av nätverkskommunikation. Finansiella enheter ska säkerställa tillgänglighet, autenticitet, integritet och konfidentialitet under överföring. Åtgärder ska införas för att förebygga och upptäcka dataläckage och säkerställa säker överföring av information.

1.8 IKT-projekt och förändringsledning

En policy för IKT-projektledning ska säkerställa effektiv hantering av IKT-projekt, inklusive riskbedömningar och säkerhetstester. Vid förändringar av IKT-system ska kontroller införas för att säkerställa att säkerhetskraven uppfylls och att ändringar implementeras på ett kontrollerat sätt. Säkerhetsrutiner ska identifiera tekniska och säkerhetsmässiga specifikationer för IKT-system. Finansiella enheter ska genomföra testning av nya och uppdaterade system innan de tas i bruk för att säkerställa att de fungerar som avsett och uppfyller säkerhetskraven.

1.9 Åtkomstkontroll

Finansiella enheter måste utveckla och införa en åtkomstkontrollpolicy som omfattar:

1. Tilldelning av åtkomsträttigheter som är baserad på behovsenlig behörighet, användning och lägsta behörighet inklusive fjärr- och nödsituationer.

2. Åtskillnad av funktioner som avser att förhindra omotiverad tillgång till kritiska data och kombinationer av åtkomsträttigheter som kan kringgå kontroller.

3. Begränsa generiska och delade användarkonton. Säkerställ identifiering av användare för utförda åtgärder i IKT-system. Det är även av betydelse att använda kontroller och verktyg för att förhindra obehörigt tillträde till IKT-tillgångar.

4. Fastställ rutiner för att bevilja, ändra eller återkalla åtkomsträttigheter snabbt vid behov eller vid anställningens slut.

5. Använda autentisering som står i proportion till IKT-tillgångars riskprofil och stark autentisering för fjärråtkomst och kritiska funktioner.

6. Loggning och övervakning av fysisk åtkomst till kritiska områden. Säkerställ att endast behöriga personer har tillgång.

1.10 IKT-relaterade incidenter

För att hantera IKT-relaterade incidenter ska finansiella enheter dokumentera incidenthanteringsprocessen, upprätta kontaktlistor med interna och externa intressenter involverade i IKT-säkerhet. De ska även använda sig av tekniska

mekanismer för att snabbt upptäcka onormal verksamhet och beteenden, bevara bevis för IKT-incidenter så länge som nödvändigt och proportionellt till incidentens allvar. Finansiella enheter ska även analysera betydande eller återkommande incidenter och identifiera mönster.

1.11 Upptäckt och hantering av incidenter

Finansiella enheter måste fastställa roller och ansvar för en effektiv upptäckt och hantering av incidenter. De ska även samla in och analysera data från interna och externa faktorer, cyberhot och incidentrapportering från tredjepartsleverantörer. Finansiella enheter bär ansvar för att effektivt hantera och upptäcka incidenter både under och utanför arbetstid. De ska även säkerställa identifiering av datum och tid för avvikande aktiviteter och skydda inspelningar mot obehörig åtkomst.

1.12 Kontinuitetshantering inom IKT

Finansiella enheter ska ha IKT-kontinuitetsplaner som inkluderar beskrivning av IKT-kontinuitetens mål, arrangemang och tidsramar. De ska inneha tydliga roller och resurser för genomförandet av kontinuitetsplanen, regelbunden testning av kontinuitetsplanen och anpassning baserat på testresultat och scenarier. Kontinuitetsplanen ska vara godkänd av ledning samt dokumenterad och tillgänglig vid nödsituationer. Kontinuitetsplanen ska även testas minst en gång om året eller vid större förändringar.

1.13 Fysisk och miljösäkerhet

Finansiella enheter ska implementera fysiska säkerhetsåtgärder baserat på hotbild och riskprofil och skydda lokaler och datacentraler från obehörigt tillträde, angrepp och miljöhot. De ska även införliva skydd mot miljöfaror genom skyddsåtgärder efter lokalernas betydelse och verksamhetens kritikalitet.

1.14 Åtkomstkontroll

Finansiella enheter ska utveckla, dokumentera och genomföra åtkomstkontroll för fysisk åtkomst. De ska även hantera användaransvar, kontohantering och autentiseringsmetoder enligt praxis. Finansiella enheter ska regelbundet granska och uppdatera åtkomsträttigheter.

1.15 Säkerhet inom IKT-verksamheten

Finansiella enheter ska övervaka IKT-tillgångars livscykel, genomföra automatiserade sårbarhetsskanningar och hantera risker med äldre eller ostödda IKT-tillgångar. De ska även logga händelser relaterade till åtkomstkontroll och IKT-drift samt genomföra åtgärder för att identifiera och analysera hot mot kritisk IKT-verksamhet. Finansiella enheter ska skydda data under användning, överföring och lagring samt förebygga obehöriga anslutningar och säkra nätverkstrafik. Det är även av betydelse att implementera procedurer för säker radering och avveckling av datalagringsenheter. De ska även utföra säkerhetstestning genom upprättande och genomförande av plan för att testa IKT-säkerhetsåtgärder regelbundet samt övervaka och utvärdera testresultaten för att uppdatera säkerhetsåtgärder.

1.16 Rapportering och översyn

Översynsrapporter ska skickas in årligen till den berörda myndigheten. Det ska skickas in en sökbar elektronisk rapport om översyn av IKT-riskhanteringsramen. Rapporten ska innehålla sammanfattningar, analys av brister och åtgärdsplaner.

2 Wesslau Söderqvist Advokatbyrås rekommendationer

För att effektivt hantera IKT-säkerhet och risker inom finansiella enheter rekommenderar Wesslau Söderqvist Advokatbyrå att finansiella enheter:

- Anpassar strategier och protokoll för nätverkssäkerhet, dataintegritet och konfidentialitet.
- Dokumenterar och implementerar riktlinjer för sårbarhetshantering, riskbedömning och krishantering. Årliga översyner av kvarstående risker är obligatoriska.
- Upprätthåller en livscykelhanteringspolicy för IKT-tillgångar inklusive kryptering och dokumentation av kritiska tillgångar.
- Säkerställer uppdatering av krypteringstekniker för att motstå cyberhot.
- Implementerar säkerhetsrutiner för installation, underhåll och återställning av IKT-system.

- Säkerställer regelbundna analyser och uppdateringar för att identifiera och hantera sårbarheter.
- Genomför åtgärder som åtkomstbegränsningar, säker konfigurationsbaslinje och skydd mot skadlig kod.
- Hanterar portabla och privata slutpunktsenheter samt säker radering av data.
- Utvecklar loggningsprocedurer för att identifiera och logga relevanta händelser och upptäcka systemfel.
- Skyddar loggar mot manipulation.
- Skyddar nätverk genom segmentering, dokumentation av nätverksanslutningar och kryptering av nätverkskommunikation.
- Förebygger och upptäcker dataläckage samt säkerställer säker överföring av information.
- Säkerställer effektiv hantering av IKT-projekt med riskbedömningar och säkerhetstester.
- Kontrollerar att säkerhetskraven uppfylls vid systemförändringar.
- Implementerar en policy för tilldelning av åtkomsträttigheter baserat på behov. Säkerställer stark autentisering för fjärråtkomst.
- Begränsar generiska och delade användarkonton samt loggar och övervakar fysisk åtkomst.
- Fastställer roller och ansvar för incidenthantering samt samlar in och analyserar data från olika källor.
- Utvecklar och testar regelbundet IKT-kontinuitetsplaner som inkluderar tydliga mål, roller och resurser.
- Implementerar fysiska säkerhetsåtgärder och skydd mot miljöfaror baserat på hotbild och riskprofil.

Rekommendationerna syftar till att stärka IKT-säkerheten, minimera risker och säkerställa kontinuitet i verksamheten för finansiella enheter.

Har ni frågor med anledning av det ovanstående eller vill ha hjälp med att implementera en riskhanteringsram i enlighet med DORA är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå.

Outlook

Nyhetsbrev - Finansinspektionen återkallar Finans 24/7 Sverige AB:s tillstånd

Från Isak Steinbach <Isak.Steinbach@wsa.se>
Datum Fre 2024-07-19 10:05
Till Kristina Jonsson <Kristina.Jonsson@wsa.se>; Johan Grenefalk <Johan.Grenefalk@wsa.se>

Hej,

Finansinspektionen har den 17 juli 2024 beslutat att omedelbart återkalla Finans 24/7 Sverige AB:s, nedan bolaget, tillstånd att driva finansieringsrörelse, på grund av att bolaget inte inom ett år från det att tillståndet beviljades börjat driva sådan rörelse som tillståndet avsett.

Enligt 2 kap. 4 § förordningen (2004:329) om bank- och finansieringsrörelse ska ett företag som fått tillstånd enligt lagen (2004:297) om bank- och finansieringsrörelse (LBF), informera Finansinspektionen om när det avser att påbörja verksamheten. Enligt 15 kap. 3 § LBF ska Finansinspektionen återkalla tillståndet om kreditinstitutet inte inom ett år från det tillstånd beviljades har börjat driva sådan rörelse som tillståndet avser. Motsvarande regler finns i fler näringsrättsliga regleringar som avser andra finansiella aktörer än kreditinstitut.

Bolaget fick tillstånd att bedriva finansieringsrörelse i oktober 2022. När Bolaget inte inkommit med någon information till Finansinspektionen om när verksamheten avsågs att påbörjas, inleddes en utredning i november 2023. Detta resulterade i att en varning sedermera utfärdades. Bolaget uppgav därvid att verksamheten planerades påbörjas under april 2024. Någon uppdatering inkom dock inte efter detta, varför Finansinspektionen påbörjade en ny utredning i juni 2024. Förseningarna uppgavs av bolaget bero på att potentiella investerare dragit sig ur processen i nära anslutning till sommarsemestrarna.

Finansinspektionen noterade att bolaget senast i oktober 2023 varit skyldigt att påbörja verksamheten och att överträdelsen av den lagstadgade tidsfristen varit betydande. Uppgifterna som lämnats under den senare utredningen ansågs inte heller tala för att verksamheten skulle kunna lanseras i närtid. Med hänsyn till den tidigare utfärdade varningen ansåg Finansinspektionen att bolagets tillstånd skulle återkallas.

Wesslau Söderqvist Advokatbyrå rekommenderar att aktörer som genom Finansinspektionen har tillstånd för verksamheter, som ännu inte har påbörjats eller är inaktiva, ser över skälet till detta. Vidare att dessa aktörer upprättar en plan för när verksamheten ska påbörjas samt underrättar Finansinspektionen om tidsplanen. Detta i syfte att undvika förseningar och administrativa kostnader som en ny tillståndsprocess kan vara förenad med. Vi vill även upplysa om att beslutet även har relevans för andra aktörer som omfattas av liknande skyldigheter såsom värdepappersbolag, fondbolag och försäkringsföretag.

Kontakta oss gärna om ni har några frågor med anledning av det ovanstående.

Med vänlig hälsning

Isak Steinbach
Biträdande jurist

WESSLAU SÖDERQVIST ADVOKATBYRÅ
Kungsgatan 36
Box 7836, 103 98 Stockholm, Sweden

Tel: +46 (0)8-407 88 00
Dir: +46 (0)8-407 88 17
Mob: +46 72-221 92 41

Outlook

Nyhetsbrev – Europeiska tillsynsmyndigheterna har offentliggjort den andra omgången policyprodukter inom ramen för DORA [WSA-AKTIV.FID451059]

Från Filippa Hörnberg <filippa.hornberg@wsa.se>
Datum Fre 2024-07-19 10:07
Till Daniel Ahlström <Daniel.Ahlstrom@wsa.se>; Kristina Jonsson <Kristina.Jonsson@wsa.se>; Johan Grenefalk <Johan.Grenefalk@wsa.se>; Sanella Petrovski <Sanella.Petrovski@wsa.se>; Mattias Örnulf <Mattias.Ornulf@wsa.se>

Hej,

De europeiska tillsynsmyndigheterna har den 17 juli 2024 offentliggjort den andra omgången policyprodukter inom ramen för DORA. Policyprodukterna innehåller fyra slutliga förslag till tekniska standarder för tillsyn, en uppsättning tekniska standarder för genomförande (ITS) och två riktlinjer. De syftar till att förbättra den digitala operativa motståndskraften inom EU:s finanssektor.

Policyprodukterna fokuserar på rapporteringsramen för IKT-relaterade incidenter, inklusive tydliga rapporteringsmallar, samt hotstyrda penetrationstester. Dessutom införs krav på tillsynsramens utformning för att stärka den digitala operativa motståndskraften inom EU:s finanssektor, vilket säkerställer kontinuerlig och oavbrutet tillhandahållande av finansiella tjänster till kunder och säkerheten för deras uppgifter.

Riktlinjerna har redan antagits av tillsynsstyrelserna för de tre europeiska tillsynsmyndigheterna. Det slutgiltiga förslaget för tekniska standarder har överlämnats till Europeiska kommissionen och de kommer att påbörja arbetet med att anta policyprodukterna inom de kommande månaderna.

Policyprodukterna inom ramen för DORA finns nu publicerade, länk till dem finns här:

ESAs published second batch of policy products under DORA (europa.eu)

Vi bevakar kontinuerligt utvecklingen på området och avser att återkomma med mer information inom kort. Kontakta oss gärna om ni har några frågor med anledning av det ovanstående.

Med vänlig hälsning

Filippa Hörnberg
Sommarnotarie

W S A
L A W

WESSLAU SÖDERQVIST ADVOKATBYRÅ
Kungsgatan 36
Box 7836, 103 98 Stockholm, Sweden
Tel: +46 (0)8-407 88 00

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. slutgiltig rapport om förslag till tekniska tillsynsstandarder och tekniska genomförandestandarder för incidentrapportering

---

25 juli 2024

1 Inledning

Den europeiska tillsynsmyndigheten (ESA) har den 17 juli 2024 offentliggjort den slutgiltiga rapporten om förslag till tekniska tillsynsstandarder (RTS) och förslag till tekniska genomförandestandarder (ITS) i enlighet med förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (DORA). I detta nyhetsbrev informerar vi om innehållet i RTS och ITS för hur incidenter ska rapporteras.

De slutgiltiga förslagen kommer att träda i kraft efter att de har antagits av Europeiska kommissionen och publicerats i Europeiska unionens officiella tidning.

För att förhindra potentiella spridningseffekter inom ramen för DORA, bör rapportering om större incidenter som lämnas in av finansiella enheter till behöriga myndigheter ge väsentlig och uttömmande information om incidenten på ett enhetligt och standardiserat sätt. Innehållet i den initiala anmälan bör begränsas till den mest väsentliga informationen för att undvika otillbörlig rapporteringsbörda för den finansiella enheten. De föreslagna ändringarna avser tidsgränser vid rapportering av den initiala anmälan, delrapporten och slutrapporten. ESA föreslår även en aggregerad rapportering på nationellt plan för finansiella enheter som endast övervakas av en behörig myndighet, förutsatt att vissa villkor är uppfyllda.

ESA har i samråd med Europeiska centralbanken och Europeiska unionens cybersäkerhetsbyrå:

- Utarbetat förslag till RTS som fastställer innehållet i rapporterna för IKT-relaterade incidenter och anmälan av betydande cyberhot samt tidsgränserna för finansiella enheter att rapportera dessa incidenter till behöriga myndigheter.

- Utarbetat förslag till ITS som fastställer standardformulär, mallar och tillvägagångssätt för finansiella enheter att rapportera en större IKT-relaterad incident eller anmäla ett betydande cyberhot.

Innehållet i RTS och ITS beskrivs ytterligare nedan.

2 Förslag till tekniska tillsynsstandarder (RTS)

Förslagen till RTS specificerar rapportering av större IKT-relaterade incidenter och anmälan om betydande cyberhot. Förslagen innehåller tidsgränser för när finansiella enheter har skyldighet att rapportera incidenterna till behöriga myndigheter. ESA:s förslag syftar till att harmonisera och effektivisera kraven på incidentrapportering och säkerställa att behöriga myndigheter får nödvändig information för att vidta tillsynsåtgärder samt förhindra spridningseffekter.

Rapporteringskrav

Finansiella enheter ska lämna tre typer av rapporter vid större incidenter, en initial anmälan, delrapport och slutrapport. Initialanmälan ska innehålla grundläggande information om incidenten och ska lämnas in snarast, senast fyra timmar efter klassificeringen av en större incident. Delrapporten ska innehålla utförligare information och lämnas in inom 72 timmar efter initialanmälan. Den slutgiltiga rapporten ska lämnas in inom en månad efter den senaste delrapporten och ska innehålla en fullständig beskrivning av incidenten samt redovisa de åtgärder som har vidtagits.

Rapporterna

Den initiala anmälan ska innehålla grundläggande information genom incidentreferenskod, upptäckts- och klassificeringstid, beskrivning av incidenten och klassificeringskriterier. Delrapporten ska bestå av datum- och tidsdetaljer för incidentens uppkomst, på vilket sätt incidenten har påverkat funktionellt område, hot och tekniker som har använts, samt information om tillfälliga åtgärder. Den slutgiltiga rapporten ska bestå av incidentens grundorsak, återställningstider, åtgärder för att förhindra framtida incidenter och ekonomisk påverkan. Rapporteringstidsgränserna syftar till att ge behöriga myndigheter effektiv information samtidigt som de finansiella enheterna får tillräckligt med tid för att hantera och rapportera incidenten på ett korrekt tillvägagångssätt. Tidsfristerna tar hänsyn till helger och bankhelgdagar och det finns undantag för mindre betydande finansiella enheter för att undvika onödig arbetsbörda.

Incidentrapportering om betydande cyberhot är frivilligt och den ska innehålla mindre omfattande information. Informationen ska inkludera hotets ursprung, potentiell påverkan och åtgärder som har vidtagits för att förhindra hotet. ESA:s förslag syftar till att skapa en enhetlig och effektiv rapporteringsstruktur för att stärka den digitala operativa motståndskraften för större IKT-relaterade incidenter och cyberhot inom EU:s finanssektor.

3 Förslag till tekniska genomförandestandarder (ITS)

ESA:s förslag fastställer tekniska standardformulär, mallar och förfaranden för hur finansiella enheter ska rapportera större IKT-relaterade incidenter och anmäla betydande cyberhot enligt DORA. Förslagen eftersträvar att harmonisera och förbättra kvaliteten på rapportering av IKT-relaterade incidenter och cyberhot inom den finansiella sektorn inom EU.

En standardiserad mall ska användas för att rapportera större IKT-incidenter i olika stadier. Finansiella enheter ska fylla i relevanta datafält i mallen för varje rapporteringsstadium och har möjlighet att fylla i informationen som krävs för senare stadier om den redan är tillgänglig. Informationen som återfinns i rapporterna måste vara korrekt. Om exakt data inte är tillgänglig vid tiden för rapportering, ska uppskattade värden baserade på tillgänglig information tillämpas. Finansiella enheter ska uppdatera tidigare lämnad information i del- och slutrapporter. Rapporterna ska lämnas genom säkra elektroniska kanaler som fastställs av den behöriga myndigheten. Om de etablerade kanalerna inte kan användas, ska finansiella enheter informera den behöriga myndigheten och använda andra säkra medel efter samråd med eller enligt tidigare överenskommelse med myndigheten. Om återkommande incidenter kumulativt uppfyller kriterierna för en större IKT-relaterad incident, ska finansiella enheter lämna aggregerad information om dessa incidenter.

Finansiella enheter som avser att låta någon annan sköta rapporteringsskyldigheten måste informera sin behöriga myndighet om det i förväg och lämna kontaktuppgifter till den tredje part som kommer att sköta rapporteringen. Tredje parts leverantörer kan skicka aggregerade rapporter om större incidenter som påverkar flera finansiella aktörer, förutsatt att vissa villkor är uppfyllda och att de behöriga myndigheterna har godkänt det.

För frivillig rapportering av betydande cyberhot ska en specifik mall användas och informationen ska vara fullständig och korrekt.

4 Wesslau Söderqvist Advokatbyrås rekommendationer

Wesslau Söderqvist Advokatbyrå rekommenderar finansiella aktörer att se över interna riktlinjer och processer för incidentrapportering. Allvarliga incidenter ska rapporteras inom fyra timmar och processen bör därför vara dokumenterad och innehålla en klar beskrivning över roller och ansvar vid en potentiell incident. Säkerställ också att IKT-avtal innehåller klausuler som ålägger IKT-leverantörer att bistå med bl.a. information vid en incident samt att IKT-leverantörer ska medverka till att begränsa potentiella skador. Wesslau Söderqvist Advokatbyrå bevakar

kontinuerligt utvecklingen för att genomföra DORA och avser att återkomma med mer information inom kort.

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

Nyhetsbrev

Ang. Finansinspektionen utfärdar sanktionsavgift på grund av överträdelse av EU:s marknadsmissbruksförordning

---

11 september 2024

1 Sammanfattning

Finansinspektionen har funnit att Niutech Group AB, nedan Bolaget, vars aktier handlas på Nordic Growth Market Nordic SME, har åsidosatt kraven i artikel 17.4 i EU:s marknadsmissbruksförordning (MAR) genom att inte underrätta Finansinspektionen om att offentliggörande av insiderinformation har skjutits upp. Vidare har Finansinspektionen funnit att Bolaget åsidosatt sina skyldigheter i artikel 18 MAR genom att inte upprätta en insiderförteckning. Bolaget ska till följd av överträdelserna betala en sanktionsavgift om 525 000 kronor.

2 Omständigheter

Under september 2023 har Finansinspektionen, inom ramen för det löpande tillsynsarbetet, begärt att Bolaget skulle inkomma med bland annat en insiderförteckning avseende den delårsrapport som Bolaget offentliggjort den 24 augusti 2023. Bolaget har uppgett att det på grund av förbiseende inte har upprättats någon insiderförteckning med anledning av delårsrapporten. Bolaget har implementerat rutiner för ändamålet och har förklarat att underlåtenheten beror på den mänskliga faktorn. I samband med detta har det även uppmärksammats att Bolaget inte heller har inkommit med någon anmälan om uppskjutet offentliggörande avseende delårsrapporten. Under Finansinspektionens utredning har det framkommit att Bolaget har beslutat att skjuta upp offentliggörandet den 11 augusti 2023, vilket var samma dag som insiderinformationen identifierades.

I programmet som Bolaget använder sig av för att upprätta insiderförteckningar finns en funktion som automatiskt anmäler uppskjutna offentliggöranden till Finansinspektionen. Den uteblivna anmälan har varit en direkt följd av att Bolaget, av förbiseende och trots sina rutiner, inte upprättat en insiderförteckning i programmet.

3 Tillämpliga bestämmelser

Enligt artikel 17.1 MAR ska insiderinformation som uppstår hos en emittent som huvudregel offentliggöras så snart som möjligt. Under vissa förutsättningar får ett uppskjutande av

offentliggörandet ske i enlighet med artikel 17.4 MAR. Om så sker ska emittenten skriftligen anmäla det till Finansinspektionen omedelbart efter offentliggörandet. Eftersom Bolaget fattat beslut om att skjuta upp offentliggörandet den 11 augusti 2023 har Bolaget varit skyldigt att informera Finansinspektionen om det uppskjutna offentliggörandet. Eftersom någon sådan anmälan inte skett har Bolaget åsidosatt de krav som gäller enligt artikel 17.4 MAR.

Enligt artikel 18 MAR ska emittenter upprätta en förteckning över alla personer som har tillgång till insiderinformation och som arbetar för dem. Insiderinformationen har uppstått i Bolaget den 11 augusti 2023 i samband med upprättandet av Bolagets delårsrapport. Bolaget har därmed varit skyldigt att upprätta en insiderförteckning avseende informationen. Eftersom någon insiderförteckning inte upprättats har Bolaget åsidosatt sina skyldigheter enligt artikel 18 MAR.

4 Finansinspektionens ingripande

Inför ingripandet har Bolaget uppgett att Bolaget ser allvarligt på det inträffade, att underlåtenheterna berott på förbiseenden och att Bolagets rutiner för hantering av insiderinformation inte har uppnått sitt syfte i det aktuella fallet. Mot bakgrund av detta har Bolaget uppgett att rutinerna ska ses över och att åtgärder vidtas för att säkerställa att liknande händelser inte inträffar igen. Bolaget har dock betonat att det inte inneburit någon vinning och att endast ett fåtal dagar förflutit från det att insiderinformationen uppstått till dess att den offentliggjorts. Under perioden har Bolaget begränsat antalet personer som fått ta del av insiderinformationen och några avvikelser i handeln har inte förekommit. Vidare har Bolagets styrelse och ledningsgrupp varit belagda med handelsförbud under den aktuella perioden.

Eftersom ett åsidosättande av artikel 17.4 och 18 MAR har skett har det funnits skäl för Finansinspektionen att ingripa mot Bolaget. Finansinspektionen får avstå från att ingripa om en överträdelse är ringa eller ursäktlig, personen i fråga gör rättelse, något annat organ har vidtagit åtgärder mot personen och dess åtgärder bedöms som tillräckliga, eller det annars finns särskilda skäl. Finansinspektionen har framhållit att det finns skäl för en restriktiv tillämpning av undantagen och att det med ringa överträdelser avses sådana som är att betrakta som bagatellartade. Exempel på ursäktliga fall är när det är uppenbart att överträdelsen begåtts av förbiseende.

Mot bakgrund av överträdelserna och vad Bolaget framfört har Finansinspektionen ansett att det inte funnits skäl att avstå från att ingripa. Det har bland annat konstaterats att det inte varit uppenbart att Bolaget begått överträdelserna av förbiseende. Överträdelserna har inneburit försämrade möjligheter för Finansinspektionen att övervaka marknaden samt varit skadliga för marknadens integritet. Att en anmälan om uppskjutet offentliggörande helt uteblivit har ansetts

allvarligare än att en anmälan kommit in för sent. På motsvarande sätt har det ansetts allvarligare att insiderförteckningen helt saknats, än om Bolaget hade upprättat en delvis bristfällig sådan.

Vid fastställande av sanktionsavgiftens storlek har det konstaterats att Bolaget har varit samarbetsvilligt under tillsynen. Bolagets finansiella ställning har inte varit sådan att den i någon riktning påverkat sanktionsavgiftens storlek och det har inte heller i övrigt funnits något som talat i försvårande eller förmildrande riktning. Mot bakgrund av Finansinspektionens sammantagna bedömning har sanktionsavgiften bestämts till 525 000 kronor.

5 Wesslau Söderqvist Advokatbyrås rekommendationer

Sanktionsbeslutet har, förutom för emittenter, även relevans för personer som handlar på emittenters vägnar eller för deras räkning eftersom dessa omfattas av skyldigheten att upprätta insiderförteckning enligt artikel 18 MAR. Bolaget i tillsynsärendet har implementerat rutiner för upprättande av insiderförteckning samt för anmälan om uppskjutet offentliggörande. Trots det och att överträdelsen varit resultatet av den mänskliga faktorn har Finansinspektionen ansett att överträdelsen inte berott på ett sådant förbiseende som annars kunde ha motiverat ett avstående från ingripande. Mot den bakgrunden rekommenderar Wesslau Söderqvist Advokatbyrå att aktörer som ska upprätta insiderförteckning implementerar processer för att säkerställa att skyldigheterna enligt MAR efterlevs. Detta för att kunna följa upp och kontrollera att de fastställda rutinerna kontinuerligt tillämpas i verksamheten. Detta gäller alla interna riktlinjer och rutiner som tillämpas i verksamheten i syfte att bibehålla god intern styrning och kontroll.

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

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. Sanktionsavgifter mot Apoteket och Apohem för överföring av personuppgifter till Meta

---

18 september 2024

1 Bakgrund

Integritetsskyddsmyndigheten (IMY) har den 29 augusti 2024 beslutat om sanktionsavgifter mot Apoteket AB, nedan Apoteket, och Apohem AB, nedan Apohem, med anledning av att bolagen använt den s.k. Meta-pixeln på sina webbplatser och överfört integritetskänsliga personuppgifter till Meta, vilket står i strid med dataskyddsförordningen (GDPR)[1].

IMY har mottagit anmälningar om personuppgiftsincidenter från Apoteket och Apohem år 2022. Vid personuppgiftsincidenterna har det överförts information om bl.a. självtester och köp av receptfria läkemedel. Omständigheterna i respektive situation har innefattat känsliga personuppgifter och det säkerhetsansvar som ställs på personuppgiftsansvarig vid behandling av kunders personuppgifter.

2 Apohem

IMY har den 14 maj 2022 mottagit en anmälan om personuppgiftsincident från Apohem. Apohem har implementerat Meta-pixeln på sin webbplats för att marknadsföra bolagets produkter på Metas plattformar vilket har resulterat i att bolaget överfört personuppgifter kopplade till ca 15 000 registrerade kunder till Meta. De som drabbats av detta är kunder som har godkänt marknadsföringskakor i Apohems samtyckeshanterare. IMY:s uppgift har varit att undersöka om Apohem hade vidtagit tillräckliga säkerhetsåtgärder och om de registrerades uppgifter utgjort känsliga personuppgifter i enlighet med GDPR. De personuppgifter som har överförts har innehållit köpinformation och kontaktuppgifter.

Personuppgiftsansvarig är primärt ansvarig för att vidta lämpliga säkerhetsåtgärder för att säkerställa att personuppgifter behandlas i enlighet med GDPR. IMY har konstaterat att Apohem har behandlat personuppgifter som står i strid med artikel 32 i GDPR, eftersom det avser uppgifter som kan härledas till b.la. hälsa och en viss person. Art. 32 i GDPR ställer krav på säkerhet i samband med behandling av personuppgifter. Kombinationen av uppgifter som förts över har gjort det möjligt att utläsa att en specifik person har köpt en viss utpekad produkt.

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Hälsa utgör känsliga personuppgifter som ges ett särskilt starkt skydd. Apohem har stridit mot bestämmelsen då bolaget enligt IMY inte har vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå för personuppgifter vid användning av analysverktyget Meta-pixeln under perioden 15 april 2021 - 26 april 2022. Behandlingen har inneburit en stor risk och krävt en hög skyddsnivå. IMY har beslutat att Apohem ska betala en administrativ sanktionsavgift om 8 miljoner kronor.

3 Apoteket

IMY har konstaterat att Apoteket inte heller har vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå för personuppgifter vid användning av analysverktyget Meta-pixeln under perioden 19 januari 2020 - 25 april 2022. Apoteket har använt sig av analysverktyget Meta-pixeln för att förbättra annonseringen mot bolagets kunder. Det har överförts känsliga personuppgifter till Meta och incidenten har uppskattningsvis påverkat 500 000 – 1 000 000 registrerade kunder. Behandling av känsliga personuppgifter kräver ytterligare säkerhetsåtgärder. IMY anser att behandlingen har inneburit en stor risk och krävt en hög skyddsnivå. Personuppgiftsansvarig är ytterst ansvarig för att säkerställa en skyddsnivå som är lämplig utifrån riskerna med behandlingen. Bedömning av lämplig skyddsnivå genomförs med beaktande av b.la. behandlingens art, omfattning, sammanhang, ändamål samt risker för fysiska personers rättigheter och friheter. IMY anser att kraven hos Apoteket brister vid behandling av känsliga personuppgifter. Apoteket har inte vidtagit tillräckliga säkerhetsåtgärder enligt IMY varför IMY har beslutat att Apoteket ska betala en administrativ sanktionsavgift om 37 miljoner kronor.

4 Wesslau Söderqvist Advokatbyrås rekommendationer

Behandling av integritetskänsliga personuppgifter innebär stora risker och ställer höga krav på bolag som behandlar sådana uppgifter. Wesslau Söderqvist Advokatbyrå rekommenderar att personuppgiftsansvariga säkerställer att behandlingen av personuppgifter är förenlig med GDPR. Det är även av betydelse att personuppgiftsansvarig är medveten om det ansvar som personuppgiftsansvarig besitter, som att bl.a. vidta tillräckliga säkerhetsåtgärder. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandlingen medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. Behandling av känsliga uppgifter ges ett särskilt starkt skydd i GDPR. Det är därför av stor betydelse att personuppgifter skyddas mot obehörigt röjande och förlust av kontroll.

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

Nyhetsbrev

Ang. Finansinspektionen ingriper mot FCG Fonder AB på grund av marknadsmanipulation

---

27 september 2024

1 Finansinspektionens sanktionsföreläggande

Finansinspektionen har den 22 augusti 2024 utfärdat ett sanktionsföreläggande mot FCG Fonder AB, nedan Bolaget, på grund av överträdelse av förbudet mot marknadsmanipulation i EU:s marknadsmissbruksförordning.

Bolaget har i december 2023 genomfört transaktioner med aktier i Profoto Holding AB och John Mattson Fastighetsföretagen AB mellan tre fonder som förvaltas av Bolaget. Vid tillfället har Bolaget placerat köp- och säljordrar via fonderna som har gått till avslut mot varandra. Transaktionerna har motsvarat 21 procent, respektive 31,7 procent, av den totala dagsomsättningen i aktierna. Finansinspektionens utredning har visat att fel har skett vid orderläggningarna, vilket har resulterat i att de har gått som vanliga limitordrar direkt till marknaden i stället för att rätteligen hanteras manuellt av den bank som vanligtvis mäklar affärer av aktuellt slag åt Bolaget. Transaktionerna har kännetecknats av att samma part samtidigt eller nästan samtidigt har lagt köp- och säljordrar med motsvarande kvantitet och pris (så kallade *improper matched orders*). Finansinspektionen anser att transaktionerna har haft eller har kunnat förväntas ge falska eller vilseledande signaler om tillgång, efterfrågan eller pris på aktierna. Mot den bakgrunden anser Finansinspektionen att Bolaget har överträtt förbudet mot marknadsmanipulation i EU:s marknadsmissbruksförordning.

Bolaget har förelagts att betala en sanktionsavgift om 200 000 kronor och har efter mottagandet av föreläggandet haft tre veckor på sig att skriftligen godkänna föreläggandet.

2 Wesslau Söderqvist Advokatbyrås rekommendationer

Sanktionsbeslutet belyser vikten av att finansiella aktörer följer regler, rutiner och processer för att undvika marknadsmanipulation. Wesslau Söderqvist Advokatbyrå rekommenderar att aktörer som i sin verksamhet utför handel med finansiella instrument på reglerade marknader, MTF-plattformar eller OTF-plattformar, ska se över sina rutiner för när transaktioner genomförs mellan två eller flera förvaltade fonder, i syfte att förebygga att transaktionerna ger missvisande signaler till marknaden. Förebyggande åtgärder kan exempelvis vara att stärka interna kontrollsystem genom t.ex. införande av kontroller, test av system och rutiner samt öka

medvetenheten och utbilda personal inom marknadsmanipulation. Det är också av stor vikt att det finns proaktiv övervakning och analys av handelsmönster. Vid upptäckta fel krävs det också att det finns en snabb åtgärdsplan som kan aktiveras och att Finansinspektionen informeras om relevant information.

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