



Till
Styrelsen i S:t Erik Försäkrings AB

Årsrapport 2023 avseende regelefterlevnad

1 Inledning

Styrelsen i S:t Erik Försäkrings AB, nedan Bolaget, har uppdragit åt Wesslau Söderqvist Advokatbyrå i Stockholm KB att upprätthålla funktionen för regelefterlevnad.

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

I avsnitt 2 nedan redovisas i sammandrag de åtgärder som funktionen för regelefterlevnad vidtagit inom ramen för ovan nämnda uppdrag under år 2023. I avsnitt 3 nedan redovisas funktionen för regelefterlevnads övergripande bedömning av Bolagets regelefterlevnad avseende perioden.

2 Händelser av relevans under året

2.1 Kontroll av Bolagets regelefterlevnad

2.1.1 Kvartal 1

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 ser över olika alternativ för att eventuellt byta ut Bolagets dataskyddsombud för att på ett enklare sätt kunna säkerställa dataskyddsombudets oberoende.

Funktionen för regelefterlevnad rekommenderar Bolaget att se över situationen med dataskyddsombudets oberoende. Dataskyddsombudet är nu att betrakta som alltför inskränkt med anledning av övriga roller i Bolagets verksamhet.

I övrigt har kontrollen inte föranlett några synpunkter.

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.

2.1.2 Kvartal 2

Outsourcing

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

Bolaget har tidigare genomfört ett arbete tillsammans med funktionen för regelefterlevnad för att se över och revidera samtliga anmälningspliktiga uppdragsavtal i syfte att säkerställa regelefterlevnad enligt ovan angivna regelverk. Framförallt har ändringar varit påkallade enligt EIOPA:s riktlinjer för molntjänster och IKT-riktlinjer. Samtliga uppdragsavtal som bedömts kritiska och viktiga för Bolagets verksamhet har anmälts till Finansinspektionen.

Utöver ovan har funktionen för regelefterlevnad informerats om att Bolagets internrevisor har haft synpunkter på den utförda kontraktsuppföljningen. Funktionen för regelefterlevnad har bedömt att Bolaget nu har goda rutiner för att följa upp sina uppdragstagare samt att uppföljning görs löpande.

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

Nya regelverk

Uppföljning och kontroll av Bolagets anpassning till dels EIOPA:s riktlinjer om informationssäkerhet, dels EIOPA:s riktlinjer om uppdragsavtal med molntjänstleverantörer. Kontrollen har syftat till att säkerställa att Bolaget har anpassat rutiner och processer efter riktlinjerna.

Som nämnts ovan har funktionen för regelefterlevnad bistått Bolaget med att anpassa verksamheten efter EIOPA:s riktlinjer. Arbetet är i princip klart, men fortsätter löpande i vissa delar avseende frågor rörande informationssäkerhet. De synpunkter som internrevisionen avgivit har i tiden efter kontrollen hanterats av Bolaget.

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

Försäkringsverksamhet

Uppföljning och kontroll avseende Bolagets regler för aktuariefunktionen. Kontrollen har syftat till att säkerställa att Bolagets riktlinjer är upprättade i enlighet med gällande regler.

Funktionen för regelefterlevnad har mottagit och granskat riktlinjerna utan några synpunkter.

Övrig regelefterlevnad

- a) Uppföljning av Bolagets efterlevnad av reglerna för försäkringstekniska avsättningar och reservsättning. Kontrollen har syftat till att säkerställa ändamålsenliga rutiner och riktlinjer i enlighet med för Bolaget gällande regler avseende dessa områden.

Bolaget har redogjort för arbetet och dess tillvägagångsätt avseende försäkringstekniska avsättningar och reservsättning. Funktionen för regelefterlevnad har vidare granskat relevanta styrdokument.

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

- b) Uppföljning av Bolagets försäkringstekniska riktlinjer. Kontrollen har syftat till att säkerställa att de försäkringstekniska riktlinjerna är ändamålsenliga och har det innehåll som krävs enligt 10 kap. 23 § FRL och 9 kap. 17, 25-26 §§ Finansinspektionens föreskrifter och allmänna råd (FFFS 2015:8) om försäkringsrörelse.

Funktionen för regelefterlevnad har mottagit och granskat Bolagets försäkringstekniska riktlinjer. Funktionen för regelefterlevnad bedömer att riktlinjerna uppfyller ovan ställda krav.

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

- c) Uppföljning och kontroll avseende Bolagets riktlinjer för återförsäkringsrisker. Kontrollen har syftat till att säkerställa att Bolagets riktlinjer är upprättade i enlighet med gällande regler.

Funktionen för regelefterlevnad har mottagit och granskat riktlinjerna utan några synpunkter.

Uppföljning av tidigare kontroller

Bolaget har tidigare informerat funktionen för regelefterlevnad om att man ser över olika alternativ för att eventuellt byta ut Bolagets dataskyddsbud för att på ett enklare sätt kunna säkerställa dataskyddsbudets oberoende.

Funktionen för regelefterlevnad har fortsatt rekommenderat Bolaget att se över situationen med dataskyddsbudets oberoende. Dataskyddsbudet är nu att betrakta som alltför inskränkt med anledning av övriga roller i Bolagets verksamhet.

2.1.3 Kvartal 3

Kunskap och kompetens

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 utbildningskravet i försäkringsdistributionsregelverket (IDD).

Bolaget har redogjort för Bolagets interna rutiner för utbildning och kunskapstest som omfattar de anställda som direkt deltar i Bolagets försäkringsdistribution. Bolaget bedöms ha goda rutiner för löpande utbildning.

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.

Riktlinjer för och uppföljning av uppdragstagare

Granskning av Bolagets interna riktlinjer för uppdragsavtal. Kontrollen har syftat till att säkerställa att Bolagets interna riktlinjer är anpassade enligt såväl FRL som EIOPA:s riktlinjer om uppdragsavtal med molntjänstleverantörer. Även EIOPA:s IKT-riktlinjer har tagits i beaktande. Därtill har Bolagets kontroll och uppföljning av uppdragstagare diskuterats. Uppföljningen utförs, dokumenteras och presenteras därefter för styrelsen i regel i slutet av året.

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

Försäkringsverksamhet

Uppföljning och kontroll av Bolagets regler för aktuariefunktionen. Kontrollen har syftat till att säkerställa att Bolagets riktlinjer är upprättade i enlighet med gällande regler.

Funktionen för regelefterlevnad har mottagit och granskat riktlinjerna utan några synpunkter.

Övrig regelefterlevnad

- a) 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 2022 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. Årets fit & proper har genomförts i slutet av september 2023.

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

- b) 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. Funktionen för regelefterlevnad har även noterat att Bolaget dessutom omfattas av Stockholm Stads riktlinjer för hantering av intressekonflikter.

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

Uppföljning av tidigare kontroller

Bolaget har tidigare informerat funktionen för regelefterlevnad om att man ser över olika alternativ för att eventuellt byta ut Bolagets dataskyddsombud för att på ett enklare sätt kunna säkerställa dataskyddsombudets oberoende.

Funktionen för regelefterlevnad rekommenderar fortsatt Bolaget att se över situationen med dataskyddsombudets oberoende. Dataskyddsombudet är nu inte att betrakta som tillräckligt oberoende med anledning av övriga roller i Bolagets verksamhet.

2.1.4 Kvartal 4

Försäkringsverksamhet

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

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

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

Övrig regelefterlevnad

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

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

- b) Uppföljning av Bolagets framåtblickande bedömning av egna risker och det egna kapitalet (ORSA). Kontrollen har syftat till att säkerställa att Bolaget ser över och genomför nödvändiga uppdateringar i Bolagets ORSA för det fall detta är påkallat. Bolaget har informerat funktionen för regelefterlevnad om att scenarier i ORSA ses över regelbundet samt att styrelsen vid sammanträde godkänt ORSA för år 2023. För år 2024 kommer ytterligare hållbarhetsscenarier vara det primära fokuset.

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

- c) Uppföljning och kontroll av etiska frågor och etiska riktlinjer. Kontrollen har syftat till att kontrollera dels att Bolaget har en process för hanteringen av etiska frågor, dels granska Bolagets riktlinjer avseende etiska frågor.

Bolaget har redogjort för processen avseende etiska frågor. Funktionen för regelefterlevnad har därtill mottagit och granskat Bolagets etiska riktlinjer.

Funktionen för regelefterlevnad har inte haft några synpunkter med anledning av

kontrollen.

Uppföljning tidigare kontroller

Bolaget har informerat funktionen för regelefterlevnad om att man ser över olika alternativ för att eventuellt byta ut Bolagets dataskyddsbud för att på ett enklare sätt kunna säkerställa dataskyddsbudets oberoende. Funktionen för regelefterlevnad avser att följa upp detta under år 2024.

2.2 Regelbevakning

Under år 2023 har funktionen för regelefterlevnad löpande informerat Bolaget om regelförändringar och löpande tillställt Bolaget nyhetsbrev. Nyhetsbrev som avser det fjärde kvartalet återfinns i sin helhet i bilaga 1, medan tidigare utskick finns återgivna sedan tidigare i respektive kvartalsrapport.

2.3 Råd och stöd

Funktionen för regelefterlevnad har löpande under år 2023 lämnat råd och stöd till Bolagets anställda avseende den tillståndspliktiga verksamheten.

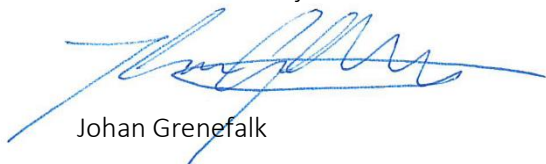
2.4 Närvaro vid styrelsesammanträden

Funktionen för regelefterlevnad har under år 2023 närvarat vid samtliga ordinarie styrelsesammanträden hos Bolaget och därvid bl.a. redogjort för funktionens rapporter.

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 19 januari 2024



Johan Grenefalk

Nyhetsbrev

Ang. Svar på konsultation om tekniska standarder till DORA

13 oktober 2023

1 Bakgrund

Wesslau Söderqvist Advokatbyrå i Stockholm KB har tidigare informerat om förordningen om digital operativ motståndskraft i den finansiella sektorn, nedan DORA, samt om utkastet till de fyra första tekniska regleringsstandarderna, nedan gemensamt benämnda RTS, som publicerats. De europeiska tillsynsmyndigheterna, EBA, EIOPA och ESMA, nedan gemensamt benämnda ESA, har publicerat en konsultation om utkastet till RTS:erna. Nedan redogörs sammanfattningsvis för några av ESA:s synpunkter och förbättringsförslag.

2 Konsultation avseende riskhanteringsramen

ESA har lämnat följande synpunkter och förbättringsförslag på RTS:en för IKT-riskhantering. Det som anges nedan är endast utdrag ur konsultationen:

- Att proportionalitetsprincipen får det genomslag som har föreslagits är lämpligt eftersom inte alla risker kan identifieras på förhand och inkluderas explicit i DORA. ESA anser dock att det är viktigt att proportionalitetskriterierna inkluderar överväganden av påverkan på kunder och användare, inte bara på den finansiella aktören som sådan.
- Det är viktigt att bedömningar av dataförlusters påverkan tar hänsyn till påverkan på kunder, användare och motparter och inte endas påverkan på den finansiella aktörens verksamhet och affärsprocesser.
- Vissa relevanta klimatrelaterade frågor (t.ex. förändringar i sannolikheten för översvämningar i områden där datacenter är belägna) har en direkt påverkan på digital operativ motståndskraft. Därför bör klimatförändringarnas fysiska påverkan identifieras. Klimatscenarier och klimatstresstester bör vägas in vid planering av affärskontinuitet och incidentåterhämtning.
- ESA vill att det tydliggörs att tilldelning av ansvar till kontrollfunktioner inte befriar verksamheten, som första försvarslinje, från ansvar.
- ESA stöder krav på dokumentation av skälen till att inte använda ledande praxis inom krypteringsteknik. Denna teknik är föremål för snabb utveckling och det kan därav vara nödvändigt och acceptabelt att i vissa fall inte använda ledande praxis.

- ESA kräver en omprövning av frekvensen för löpande utbildning inom IKT. ESA anser att krav på minst årlig utbildning anses för frekvent.

3 Konsultation avseende klassificering av IKT-relaterade incidenter

ESA har lämnat följande synpunkter och förbättringsförslag på RTS:en för klassificering av IKT-relaterade incidenter. Det som anges nedan är endast utdrag ur konsultationen:

- Enligt DORA ska finansiella aktörer som ett kriterium för att klassificera IKT-relaterade incidenter beakta bl.a. antalet kunder som påverkas. ESA påpekar att även varaktighet av påverkan ska beaktas. Händelser som påverkar ett stort antal kunder men som har mycket kort varaktighet (här är det frågan om sekunder eller minuter) bör enligt ESA inte nödvändigtvis rapporteras om de inte innebär någon påverkan på kunderna.
- RTS:en kräver att finansiella aktörer mäter varaktigheten av en incident "från det ögonblick då incidenten inträffar". Eftersom detta i praktiken kan vara svårt att specificera, beroende på omständigheterna, anser ESA att formuleringen bör ersättas med "från det ögonblick då incidenten upptäcktes".
- ESA önskar klargöranden kring hur det ska avgöras vid vilken tidpunkt som en incident anses ha upphört och när aktiviteter ska anses ha återställts till den nivå av service som tillhandahölls i tiden innan incidenten. Det bör förtydligas om det är tillräckligt att orsaken till en incident har åtgärdats temporärt eller om det krävs en permanent lösning för att verksamheten som drabbats ska anses vara återställd.
- ESA anser att tröskeln för att definiera "ekonomisk påverkan", som uppgår till 100 000 EUR eller mer, är för lågt satt med tanke på kostnaderna för att hantera större incidenter. Vidare bör det beaktas att finansiella aktörer kan stöta på betydande utmaningar när specifika detaljer om den ekonomiska påverkan ska samlas in i det ögonblick då incidenten upptäcks (vilket också är tidpunkten då incidenten måste rapporteras). Därför kan det vara svårt att korrekt fastställa om tröskeln för detta kriterium har uppfyllts.
- Förlorade eller komprometterade personuppgifter kan orsaka betydande följdskador, t.ex. bedrägerier, och personuppgifter åtnjuter särskilt skydd enligt GDPR. IKT-system som hanterar personuppgifter bör därför uppfylla högsta standard av säkerhet. ESA anger dessutom att dessa system bör ägnas särskild uppmärksamhet av tillsynsmyndigheter.
- ESA belyser vikten av att tillsynsmyndigheternas rapporteringskrav i DORA upprätthålls för att undvika dubbelrapportering med beaktande av NIS2.



4 Wesslau Söderqvist Advokatbyrås rekommendationer

DORA syftar till att förbättra den digitala operativa motståndskraften för finansiella aktörer. DORA täcker viktiga områden som riskhantering, hantering och rapportering av IKT-relaterade incidenter, testning av digital operativ motståndskraft samt hantering av IKT-tredjepartsrisk.

Det är av största vikt att göra en riskanalys för att veta var resurser behövs och vilka åtgärder som behöver vidtas. Att inte göra någon riskanalys är en betydande risk i sig. DORA ska börja tillämpas från den 17 januari 2025. Till dess behöver finansiella aktörer åtminstone ha identifierat och minimerat de största riskerna. Det ska även vid denna tidpunkt finnas ändamålsenliga rapporteringsrutiner på plats och för detta ändamål måste det även finnas rutiner för att klassificera incidenter. Dessutom behöver finansiella aktörer veta hur de på bästa sätt ska övervaka IKT-leverantörer och stresstesta IKT-system.

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

Nyhetsbrev

Ang. Ny lag om granskning av utländska direktinvesteringar

9 november 2023

1 Bakgrund

Den 13 september 2023 antog riksdagen en ny lag om granskning av utländska direktinvesteringar.¹ Lagen implementerar ett EU-direktiv och träder i kraft den 1 december 2023. Lagen syftar till att hindra utländska direktinvesteringar i svensk skyddsvärd verksamhet som kan inverka skadligt på Sveriges säkerhet eller på allmän ordning eller allmän säkerhet i Sverige. Lagen ska således täcka behovet av att kunna kontrollera och, när det bedöms nödvändigt, förhindra utländska investerares uppköp och strategiska förvärv av vissa inhemska företag.

Den nya lagen uppställer en omfattande anmälningsskyldighet för investerare då planerade investeringar över en viss angiven gräns kommer att kräva en anmälan till granskningsmyndigheten, Inspektionen för strategiska produkter, nedan ISP.

Myndigheten för samhällsskydd och beredskap, nedan MSB, får meddela föreskrifter om vilka samhällsviktiga verksamheter som ska omfattas av den nya lagen.² Även de föreskrifterna planeras att träda i kraft den 1 december 2023.

Nedan redogörs närmare för vad den nya lagen innebär för de som omfattas av den samt vilka åtgärder som bör vidtas innan lagen träder i kraft den 1 december 2023.

2 Lagen om granskning av utländska direktinvesteringar

2.1 Skyddsvärd verksamhet

Lagen syftar, som tidigare nämnts, till att förhindra utländska direktinvesteringar i skyddsvärda verksamheter som kan vara skadliga för Sveriges säkerhet. I lagen finns en exemplifierande lista över vad som utgör verksamheter av intresse för svenska säkerhetsintressen och som således är skyddsvärda, t.ex. anges samhällsviktig verksamhet. Exempelvis anges banker, livförsäkringsbolag, pensionsfondverksamhet och administrativa tjänster till finansiella marknader som exempel i föreskrifterna. Det är dock inte klart vad som avses med

¹ Lag (2023:560) om granskning av utländska direktinvesteringar.

² Förordning (2023:624) om granskning av utländska direktinvesteringar.

”administrativa tjänster”. Även säkerhetskänslig verksamhet och behandling i stor omfattning av känsliga personuppgifter i eller genom en vara eller tjänst ska anses vara skyddsvärd verksamhet.

Remisstiden för de nya föreskrifterna om skyddsvärd verksamhet gick ut den 3 november 2023. Definitionerna kan således komma att ändras.

2.2 Anmälningsskyldighet

Den som har för avsikt att direkt eller indirekt investera i en skyddsvärd verksamhet åläggs en skyldighet att, innan investeringen genomförs, anmäla sin investering i skyddsvärd verksamhet till ISP bl.a. när denne får kontroll över 10, 20, 30, 40, 65 eller 90 procent av rösterna. Detta innebär att parterna kan träffa ett avtal om investeringen innan en anmälan görs men att fullföljandet behöver villkoras av att ISP lämnar anmälan om investeringen utan åtgärd eller godkänner investeringen. ISP ska meddela ett beslut inom 25 arbetsdagar från det att en fullständig anmälan kommit in. Om en sådan investering saknar tredjelandsimpplikationer kommer ISP meddela att man lämnar anmälan utan åtgärd och det är då tillåtet att genomföra investeringen. ISP kan även inleda en granskning av investeringen och beslut om godkännande eller förbud ska då lämnas inom tre månader som utgångspunkt. Observera att det krävs ett beslut om att anmälan lämnas utan åtgärd oavsett att man vet att sådana tredjelandsimpplikationer saknas, så länge investeringen sker i en skyddsvärd verksamhet och överstiger något av de angivna gränsvärdena.

Ett företag som är föremål för en investering som är anmälningspliktig ska i huvudregel även upplysa investeraren om anmälningsskyldigheten.

Av förarbetena framgår att ett moderbolag i en koncern får anses indirekt förfoga över röster som ett dotterbolags förvärv av aktier motsvarar. Det innebär att de investeringar som görs inom en koncern ska räknas samman när det gäller att avgöra om ett gränsvärde har uppnåtts.

Vid en överträdelse av regelverket har ISP rätt att ta ut en sanktionsavgift upp till högst 100 000 000 kronor.

2.3 Investerare

Lagen anger ingen definition av termen *investerare*. Flera remissinstanser är kritiska till att investeringar som ska genomföras av svenska aktörer ska omfattas av anmälningsplikt. För att reglerna inte ska kunna kringgås gäller dock denna anmälningsskyldighet för samtliga



investerarare, oavsett investerarens nationalitet eller säte. Därmed omfattas svenska investerare av reglerna.

2.4 Särskilt om fondbolag

Även fondbolag omfattas av anmälningsplikten och måste göra en anmälan till ISP så fort en investering medför att gränsvärdet om 10 procent kommer att överstigas. Dessvärre saknas det någon närmare analys av hur den nya lagen ska förhålla sig till svensk finansiell lagstiftning. Fondbolag gör dagliga transaktioner i mycket stor omfattning och det saknas analys av hur en anmälningsplikt kan påverka denna handel. Påverkan kan bli väldigt stor om transaktioner kan genomföras först efter 25 dagar, då ISP *eventuellt* ger ett beslut som tillåter ett genomförande.

3 Wesslau Söderqvist Advokatbyrås rekommendationer

Wesslau Söderqvist Advokatbyrå rekommenderar att investerare som framgent kan komma att investera i skyddsvärd verksamhet utarbetar en rutin för att säkerställa att den nya lagen efterlevs på ett ändamålsenligt sätt. Framtida investeringar som kan tänkas överskrida något av gränsvärdena bör ses över. Det behöver ses över om sådana investeringar är tänkta att genomföras i ett portföljbolag som bedriver någon verksamhet som är skyddsvärd. Sådana investeringar ska i sådana fall, fr.o.m. den 1 december 2023, anmälas till ISP för beslut innan de kan genomföras.

Det är viktigt att komma ihåg att gränsvärdet om 10 procent även avser indirekt ägande vilket gör att investeringar inom en koncern ska räknas samman.

Wesslau Söderqvist Advokatbyrå avser att följa utvecklingen av den nya lagen och de föreslagna föreskrifterna.

Har ni frågor med anledning av det ovanstående, eller behöver hjälp med att utreda hur just ert bolag kan anpassa sig till reglerna, är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå.



Nyhetsbrev

Ang. IMY:s föreskrifter om behandling av personuppgifter som rör lagöverträdelser

22 november 2023

1 Inledning

Vid behandling av personuppgifter med digital teknik eller om personuppgifter samlas in för att lagras i ett digitalt system ska GDPR efterlevas. Den som behandlar personuppgifter, nedan personuppgiftsansvarig, ska bl.a. ska fastställa för vilka ändamål behandlingen sker. Personuppgiftsansvarig ska endast behandla de uppgifter som krävs för det fastställda ändamålet, s.k. uppgiftsminimering.

Det finns en rad bestämmelser som de europeiska medlemsstaterna själva kan reglera inom ramen för personuppgiftshanteringen. Ett sådant område är behandling av personuppgifter som rör fällande domar i brottmål. IMY har nu tagit fram ett förslag med föreskrifter för när det ska vara tillåtet för andra än myndigheter att behandla sådana personuppgifter. Föreskrifterna ska tillämpas av bl.a. företag under Finansinspektionens tillsyn som dessutom är skyldiga att efterleva lagen om åtgärder mot penningtvätt och finansiering av terrorism, nedan penningtvättsregelverket.

2 Förslag om nya föreskrifter från IMY

De nya föreskrifterna medför att företag under Finansinspektionens tillsyn som är skyldiga att efterleva kraven i penningtvättsregelverket får behandla personuppgifter avseende fällande domar i brottmål för kontroller mot sanktionslistor. Resultatet av om förslaget går igenom är att dessa finansiella företag inte längre behöver ansöka om tillstånd för att använda sanktionslistor.

För att behandlingen ska få genomföras krävs det att

- 1) sanktionslistorna är fastställda i demokratisk ordning och är allmänt tillgängliga på utfärdande myndigheters eller mellanstatliga organisationers webbplatser, och
- 2) den personuppgiftsansvariga vidtagit relevanta skyddsåtgärder för att kunna skilja på äkta och falska träffar.

Dessutom får personuppgiftsbehandling enligt första stycket endast avse i) företagets befintliga och presumtiva kunder, ii) leverantörer, iii) samarbetspartners, iv) förmedlare, v) arbetstagare och arbetssökande, vi) uppdragstagare, vii) styrelsemedlemmar, fullmaktshavare,

ställföreträdare eller firmatecknare, viii) ägare och verkliga huvudmän, tredjemanspantsättare och borgensmän, ix) motparter i en transaktion samt därmed jämförliga kategorier av personer.

Om de ovan nämnda rekvisiten är uppfyllda, får alltså behandling av personuppgifter avseende fällande domar i brottmål ske.

De slutgiltiga föreskrifterna är ännu inte beslutade. Finansinspektionen har nyligen uttalat sig om förslaget. Finansinspektionen tillstyrker i huvudsak förslaget men anser att alla finansiella företag ska kunna använda sig av sanktionslistorna, inte bara de som omfattas av penningtvättsregelverket.

3 Wesslau Söderqvist Advokatbyrås rekommendationer

Wesslau Söderqvist Advokatbyrå rekommenderar företag under Finansinspektionens tillsyn som är skyldiga att efterleva kraven i penningtvättsregelverket att ta kravet på att sanktionslistor ska vara demokratiskt fastställda i beaktande. Det ska dessutom finnas rutiner och processer för att kunna skilja på äkta och falska träffar i sanktionslistor. Det måste även säkerställas att de uppgifter som behandlas är sådana som avser den godkända kretsen ovan, se i) - ix). Tänk även på att behandlingen i enlighet med de nya föreskrifterna dessutom kan påverka personuppgiftsregistret och att de interna regeldokumenterna kan behöva ses över.

En positiv konsekvens av föreskrifterna är att finansiella företag som är skyldiga att efterleva kraven i penningtvättsregelverket inte kommer att behöva ansöka om tillstånd för att använda sanktionslistor.

Wesslau Söderqvist Advokatbyrå delar Finansinspektionens uppfattning i frågan varför föreskrifterna ska vara avgränsade till att gälla företag som är skyldiga att efterleva kraven i penningtvättsregelverket. Det är oklart vilka hinder som anses föreligga för att alla finansiella företag ska kunna använda sig av sanktionslistorna. Wesslau Söderqvist Advokatbyrå avser att bevaka området och eventuella förändringar avseende föreskrifternas tillämplighet.

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



Nyhetsbrev

Ang. Cookies

23 november 2023

1 Post- och telestyrelsens nya riktlinjer

Den 26 juni 2023 har Post- och telestyrelsen, nedan PTS, underrättat Tele2, Swedbank, Folkhälsomyndigheten samt Konsumentverket misstanke om bristande efterlevnad av bestämmelsen om cookies. Aktörerna har meddelats en rad åtgärder som de förväntats att vidta för att uppfylla kraven i regelverket. Dessa åtgärder redogörs för nedan, eftersom de i någon mån kan anses vara vägledande.

Cookies är små datafiler som används för att lagra information eller få åtkomst till information som finns lagrad i en användares dator eller mobil. Cookies kan minnas en användares webbaktivitet, t.ex. inloggningsuppgifter, språkställningar eller skräddarsydd marknadsföring. I svensk rätt finns det en mängd regler att beakta vid hantering av cookies på en webbsida.

För att uppgifter som lagras genom cookies ska få behandlas krävs det att den vars uppgifter behandlas får tillgång till information om ändamålet för behandlingen samt lämnar samtycke till behandlingen. Viss typ av behandling av cookies får emellertid ske även om förutsättningarna inte är uppfyllda. Sådan behandling omfattar behandling som krävs för överföring av ett elektroniskt meddelande via ett elektroniskt kommunikationsnät (typiskt sett sociala medier) och behandling som är nödvändig för en tjänst som användaren uttryckligen har begärt.

Vad som är samtycke ska avgöras på likartade grunder som vid hanteringen av en personuppgift enligt Dataskyddsförordningen (GDPR). Med samtycke avses därmed varje slag av frivillig, specifik, informerad och otvetydig viljeyttring genom vilken den registrerade godkänner behandling av personuppgifter som rör denne. Samtycket kan återkallas när som helst.

PTS har, som redogjorts för ovan, specificerat ett antal åtgärder som krävs för att en verksamhet ska vara förenlig med bestämmelsen om cookies. Dessa åtgärder är inte uttömmande, utan ska uppfattas som exemplifierande. Först och främst menar PTS att det ska vara möjligt för användare att neka till lagring av inte nödvändiga cookies på ett lika enkelt sätt och vid samma tillfälle och i samma vy som användare ges möjlighet att lämna samtycke till behandlingen.



För att säkerställa att frivilliga samtycken inhämtas ska färger och kontraster användas på ett sätt som inte framhäver alternativ för att lämna samtycke framför alternativ att neka samtycke. Dessutom ska information ges om att det finns en rätt att när som helst återkalla det samtycke som givits. Därutöver krävs det att det ska vara lika lätt att återkalla som att ge samtycke. Slutligen krävs även att inte nödvändiga cookies specificeras och redovisas för respektive behandling.

2 Wesslau Söderqvist Advokatbyrås rekommendationer

Wesslau Söderqvist Advokatbyrå rekommenderar att verksamhetsutövare tar del av och beaktar PTS:s riktlinjer avseende cookies för att säkerställa överensstämmelse med regelverket. Det innebär att webbplatsen bör erbjuda en enkel och tydlig möjlighet för användare att neka lagring av inte nödvändiga cookies vid samma tillfälle och i samma vy som samtycke ges. Dessutom betonas vikten av att undvika framhävande färger på godkännandeknappen, informera om rätten att återkalla samtycke och göra processen för återkallelse lika lätt som att ge samtycke.

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



Nyhetsbrev

Ang. IMY har utfärdat sanktionsavgift mot Indecap AB

12 december 2023

1 Bakgrund

Integritetsskyddsmyndigheten, nedan IMY, har i januari 2021 mottagit klagomål angående att fonrådgivaren Indecap AB, nedan Indecap, felaktigt skickat ett e-postmeddelande innehållande en fil med personuppgifter om bl.a. kunders ekonomi till andra kunder. IMY har med anledning av klagomålen inlett tillsyn mot Indecap för att utreda det som framgår av klagomålen.

Det som inträffat i det aktuella fallet är att en medarbetare på Indecap hämtat ut information ur ett skyddat system för att bearbeta till en rapport i Excel. Excelfilen har därefter döpts till ett namn som liknat namnet på den PDF-rapport över fondernas utveckling som varit menad att skickas ut till kunder. När den korrekta PDF-rapporten skulle skickas ut till kunderna har medarbetaren i stället råkat bifoga Excelfilen som innehållit diverse personuppgifter om kunder.

IMY har efter genomförd utredning konstaterat att Indecap på grund av incidenten har behandlat personuppgifter i strid med artikel 32.1 i GDPR. IMY har i sitt beslut den 7 november 2023 meddelat att Indecap skulle åläggas att betala en administrativ sanktionsavgift om 500 000 kronor för överträdelsen. Nedan redogörs för de skäl som ligger bakom beslutet samt vilka åtgärder som Wesslau Söderqvist Advokatbyrå rekommenderar med anledning av beslutet.

2 Indecaps rutiner för personuppgiftshantering

Indecap har haft en informationssäkerhetspolicy på plats och tillämpat dokumenterade processer och rutiner kopplade till personuppgifts- och informationssäkerhetshantering. Innan incidenten inträffade hade Indecap behörighetsbegränsat de aktuella system som berör kunduppgifter så att endast fyra medarbetare hade tillgång till dessa. Indecap hade vidare utbildat samtlig personal i personuppgifts- och informationssäkerhetshantering.

Indecap har efter incidenten genomfört en internutredning där bolaget noterat svårigheter med att efterleva dualitetsrutinen vid större hantering av personuppgifter. Rutinen har inneburit att två personer skulle godkänna/verifiera en viss handling innan den fick genomföras. Det har dock varit problem med att genomföra detta då flera arbetat hemifrån sedan pandemin och rutinen inte har gått att genomföra digitalt.



Indecap har även en systembaserad applikation med inloggning via BankID i syfte att minska riskerna som uppstår när uppgifter skickas via e-post. Ett beslut om att sluta skicka utskick via e-post och i stället hänvisa kunder till att logga in med BankID hade fattats innan incidenten men hade inte hunnit genomföras. Numera hänvisas alltså kunderna till att logga in med BankID för att se sin portföljutveckling och rapporter innehållande kunduppgifter är krypterade och lösenordskyddade.

Därutöver har Indecap bl.a. uppdaterat rutinerna kring hemarbete och dualitetsprocessen, skickat information till kunderna om det inträffade samt vidtagit ytterligare tekniska säkerhetsåtgärder och hållit extra utbildningsinsatser för anställda.

3 IMY:s utredning och motivering till beslut

3.1 Behandlingen har inneburit en hög risk

Genom IMY:s utredning har det framkommit att den av Indecap av misstag skickade okrypterade PDF-filen innehållit personuppgifter om ca 52 000 kunder. E-postmeddelandet har skickats till ca 2 800 mottagare som inte varit behöriga att motta den aktuella informationen. Den skickade filen har bl.a. innehållit uppgifter om kunders namn, e-postadresser, personnummer, bank, risknivå, enskilt fondval och det senast inlästa värdet av kundens innehav i fonder.

IMY har inledningsvis konstaterat att Indecap har en skyldighet att skydda de personuppgifter som bolaget behandlar genom att vidta lämpliga tekniska och organisatoriska åtgärder. De åtgärder som vidtas ska säkerställa en lämplig säkerhetsnivå. IMY påpekar att Indecap är ett värdepappersbolag varför det därutöver finns lagstadgade krav om tystnadsplikt i verksamheten. Mot bakgrund av det menar IMY att det ställs särskilt höga krav på skydd för de personuppgifter som behandlas i verksamheten.

Det har dessutom varit fråga om en behandling av personuppgifter som varit särskilt skyddsvärda eftersom det bland uppgifterna som spridits funnits personnummer. Det har dessutom avsett uppgifter till ett stort antal kunder. Sammantaget har behandlingen således inneburit en hög risk.

3.2 Indecap har inte vidtagit tillräckliga åtgärder

IMY har gjort bedömningen att det aktuella misstaget hade kunnat hindrats eller åtminstone försvårats. Indecap borde ha haft tydliga rutiner för att säkerställa att hanteringen av skyddsvärd information inte skulle sammanblandas med hanteringen av publik information. Det



faktum att filen med skyddsvärd information har döpts till ett namn snarlikt filen med publik information menar IMY talar för att tillräckligt tydliga instruktioner saknats.

Det har inte heller framkommit något som tyder på att Indecap har haft några tekniska eller organisatoriska hinder eller kontrollfunktioner som har försvårat hanteringen av filen, t.ex. tekniska hinder eller varningar, i samband med att filen bifogats som e-post. Den rutin som Indecap har haft på plats har varit den dualistiska som bolaget självt uppgivit inte har fungerat på grund av pandemin och hemarbetet under perioden. IMY har i samband med detta konstaterat att det inte är en tillräcklig ursäkt med tanke på den skyddsnivå som konstaterats för de aktuella uppgifterna. Indecap borde ha ersatt befintliga säkerhetsrutiner med likvärdigt skydd.

PDF-filen har inte varit krypterad eller innehållit någon form av läs begränsningar. Det har dessutom funnits en risk för att uppgifterna skulle spridas vidare.

Sammantaget har IMY konstaterat att Indecap inte har vidtagit tillräckliga tekniska och organisatoriska åtgärder i enlighet med GDPR för att säkerställa en säkerhetsnivå som varit lämplig i förhållande till risken.

4 Wesslau Söderqvist Advokatbyrås rekommendationer

Wesslau Söderqvist Advokatbyrå rekommenderar att personuppgiftsansvariga ser över processer och riktlinjer avseende hantering av personuppgifter. En lämplig säkerhetsnivå ska kunna säkerställas för varje behandling av personuppgifter som utförs. Vid en översyn bör särskilt sådana processer som innebär behandling av känsliga personuppgifter beaktas.

Precis som vid tidigare utskick när IMY har meddelat sanktionsavgifter på grund av överträdelser av GDPR vill vi påminna om att vad som utgör en lämplig säkerhetsnivå är olika från en personuppgiftsansvarig till en annan. En lämplig säkerhetsnivå kan variera i förhållande till behandlingens art, omfattning, sammanhang och ändamål varför det är lämpligt att varje personuppgiftsansvarig gör en skraddarsydd analys av sin verksamhet och anpassar rutinerna för personuppgiftsbehandling efter riskanalysen.

IMY har också i detta beslut konstaterat att pandemin inte utgör en giltig ursäkt för att tidigare rutiner inte fungerar som de ska. Det är ett tydligt exempel på att riskanalysen bör ses över löpande och anpassas efter mängden och typen personuppgifter som hanteras i verksamheten.

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

Nyhetsbrev

Ang. Varning och sanktionsavgift mot Aros Kapital AB

20 december 2023

1 Bakgrund

Finansinspektionen har i november 2020 inlett en undersökning av om kreditmarknadsbolaget Aros Kapital AB nedan Aros, i sin kreditgivning har följt tillämpliga regelverk i sina styrdokument, i sin organisationsstruktur och kreditprocess samt i sin interna rapportering och uppföljning. Då Finansinspektionen vid denna inledande undersökning påträffat ett flertal brister har undersökningen utökats till att utöver kreditriskhanteringen även omfatta Aros åtgärder mot penningtvätt och finansiering av terrorism, beräkning och rapportering av kreditrisker, bruttosoliditetsgrad och stora exponeringar samt Aros styrning, riskhantering och kontroll av dessa områden. Ett flertal brister har identifierats vilket medfört att Finansinspektionen beslutat att meddela Aros en varning förenad med en sanktionsavgift om 45 000 000 kronor.

Nedan redogörs närmare för de brister som Finansinspektionen identifierat.

2 Finansinspektionens undersökning

2.1 Kreditriskhantering

I den första delen av undersökningen har Aros kreditriskhantering granskats genom stickprov avseende perioden 1 april 2018 - 31 december 2021. De granskade beslutsunderlagen har legat till grund för Aros beslut om ursprunglig kredit, höjning av kreditbelopp, villkorsändringar och omprövningar. Enligt lagen (2004:297) om bank- och finansieringsrörelse (LBF), måste kreditinstitut, innan de beviljar en kredit, bl.a. noggrant pröva risken för att förpliktelseerna enligt kreditavtalet inte kan fullgöras. Det som anges i LBF preciseras genom Finansinspektionens föreskrifter och allmänna råd (FFFS 2018:16) om hantering av kreditrisker i kreditinstitut och värdepappersbolag.

Flera av Aros beslutsunderlag för kreditbeslut har visat sig ha betydande brister.

Finansinspektionen har påpekat att kreditprövningarna inte varit tillräckligt noggranna eller av tillräcklig kvalitet, vilket utgjort en risk för Aros stabilitet. Det har vidare framkommit att relevant information, både historisk och framåtblickande, saknats i många underlag. Aros har inte heller uppdaterat beslutsunderlagen när ny information tillkommit som kunde ha varit avgörande för kredittagarens återbetalningsförmåga.

Aros har hävdats att det i vissa fall kan vara så att information har beaktats i bedömningen men inte dokumenterats. Finansinspektionen menar att avsaknaden av dokumenterade analyser inte enbart beror på bristande dokumentation utan snarare på att Aros inte alls genomfört de analyser och bedömningar som krävts.

Vid utlåning till företag krävs en känslighetsanalys av kredittagarens återbetalningsförmåga och säkerheternas värdeförsämring. Finansinspektionen har noterat att det i vissa beslutsunderlag helt saknas sådana analyser samt att Aros i vissa fall hänvisat till indikationer på att analyser genomförts, vilket Finansinspektionen inte ansett tillräckligt.

Enligt kreditriskföreskrifterna ska kreditgivare om det behövs genomföra samlimitering för att beakta den samlade riskbilden för alla kunderna i gruppen samt hur anknytningen påverkar återbetalningsförmågan. Finansinspektionen har konstaterat att dokumenterad information om samlimitering saknats i majoriteten av de granskade stickproven. Aros har invänt att bolaget inte har brutit mot föreskrifterna då flera fall som Finansinspektionen hänvisar till avsett beslut om klientlimiter i samband med fakturaköp och därmed inte omfattas av kravet.

Finansinspektionen har emellertid hävdats att även om slutkundens betalningsförmåga är av störst betydelse vid sådana fakturaköp så medför inte det att förhållanden vad gäller kredittagaren kan ignoreras.

2.2 Penningtvätt

Finansinspektion har vidare utrett om Aros efterlevt bestämmelserna avseende allmän riskbedömning, riskbedömning av kunder, rutiner för valideringsprocessen samt åtgärder för kundkännedom i lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism samt Finansinspektionens föreskrifter (FFFS 2017:11) om åtgärder mot penningtvätt och finansiering av terrorism.

Vad gäller den allmänna riskbedömningen har Finansinspektionen konstaterat att flera av Aros kunder har bedrivit handel med mobiltelefoner, en vara som är vanligt förekommande i momsbedrägerier. Som tidigare nämnts är en av de produkter som Aros erbjuder sina kunder fakturaköp (factoring). Finansinspektionen framhäver i sitt beslut att det inom den organiserade brottsligheten i hög utsträckning förekommer brottsliga upplägg för att tvätta pengar där finansierings- och factoringföretag är inblandade. Trots att Aros visat medvetenhet om riskerna anser inte Finansinspektionen att bolaget tillräckligt beaktat dem i sin allmänna riskbedömning. Aros har även visat brister i rapporteringen av misstänkta aktiviteter till Polismyndigheten.

Vad gäller riskbedömning av kunder och valideringsprocesser har Aros använt en riskklassificeringsmodell för att bedöma penningtvättsrisken hos kunder. Finansinspektionen

anser att modellen närmast systematiskt medfört att högrisk kunder bedömts som låg- eller medelrisk kunder på grund av det mycket begränsade genomslaget som Aros gett högriskfaktorer.

Finansinspektionen har vid granskningen av kundakter noterat att det i 25 av 70 undersökta akterna funnits transaktioner som genererat larm i övervakningssystemet. Finansinspektionen har dock inte funnit underlag för att Aros med anledning av larmen kontrollerat och säkerställt att Aros kundkännedom om kunden varit aktuell och tillräcklig för att hantera den bedömda risken för penningtvätt eller finansiering av terrorism. Vidare har framkommit att Aros inte adekvat har vidtagit skärpta åtgärder för högrisk kunder och har brustit i att samla in tillräcklig information om affärsförbindelser samt källan till kunders medel, vilket är avgörande för att hantera situationer med hög risk för penningtvätt och finansiering av terrorism

2.3 Tillsynsförordningen och genomförandeförordningen

Aros har brutit mot tillsynsförordningen och genomförandeförordningen genom att på ett felaktigt sätt rapportera felaktiga finansiella uppgifter. Överträdelserna har medfört att Aros har rapporterat in felaktiga uppgifter om sin finansiella ställning till Finansinspektionen och att bolaget inte har rapporterat enligt de instruktioner och specifikationer som finns i genomförandeförordningen. Denna felaktiga rapportering har påverkat bedömningen av kreditrisker och stora exponeringar negativt, vilket underminerat Aros faktiska finansiella ställning.

2.4 Styrning och riskhantering

Granskningen har avslöjat fem huvudsakliga brister i Aros styrning, riskhantering och kontroll av områdena nämnda i 2.1 – 2.2. ovan. Dessa har inkluderat målsättning och rapporteringsproblem, ett otillräckligt riskhanteringsramverk, bristfälliga resurser och bristfälligt oberoende inom kontrollfunktionerna samt brister i internrevisionen som medfört att planerade aktiviteter inte kunnat genomföras. Styrelsens ansvar och åtgärder beträffande identifierade problem har dessutom ansetts vara otillräckliga och för sent införda.

3 Finansinspektionens bedömning

I ljuset av dessa allvarliga överträdelser, trots att inga konkreta skador rapporterats, har Finansinspektionen beslutat att utfärda en varning till Aros och ålagt bolaget en betydande sanktionsavgift om 45 000 000 kronor. Finansinspektionen har erkänt att Aros vidtagit åtgärder för att adressera bristerna och minska framtida risker, men betonat allvaret i överträdelserna och deras potentiella inverkan på förtroendet för det finansiella systemet.

4 Wesslau Söderqvist Advokatbyrås rekommendationer

Wesslau Söderqvist Advokatbyrå rekommenderar att kreditgivare och även andra finansiella företag mot bakgrund av Finansinspektionens beslut särskilt ser över följande punkter.

- **Kreditriskhantering:** Företag som tillhandahåller krediter bör noggrant granska och kontinuerligt förbättra sina kreditprövningsprocesser. Beslutsunderlag ska hållas uppdaterade och noggranna analyser ska genomföras för att bedöma kreditrisker.
- **Penningtvättsåtgärder:** Företag ska löpande genomföra en riskbedömning för att identifiera och hantera potentiella risker. Dessutom är det viktigt att säkerställa adekvat rapportering av misstänkta aktiviteter och transaktioner. Särskild uppmärksamhet bör riktas mot kunder och produkter som är föremål för högre risk.
- **Säkerställ korrekt rapportering:** Företag bör se över sina rapporteringsrutiner och försäkra sig om att de överensstämmer med externa regler. En noggrann och korrekt redovisning av finansiell ställning är avgörande för att undvika felaktig bedömning av kreditrisker och stora exponeringar.
- **Optimera riskhanteringsramverk:** Det är kritiskt att företag har ett robust och integrerat riskhanteringsramverk. Detta inkluderar en effektiv riskklassificeringsmodell och valideringsprocess. Företag bör se över och anpassa sina modeller för att bättre reflektera de faktiska riskerna i deras verksamhet.
- **Stärk interna kontroller och öka oberoende:** Företag bör investera i sina interna kontrollfunktioner och se till att de har tillräckliga resurser och oberoende.
- **Tydlig kommunikation med styrelsen:** Det är viktigt att rapportera såväl framgångar som motgångar så att styrelsen har en realistisk bild av företagets verksamhet och kan fatta välgrundade beslut.

Genom att följa dessa rekommendationer kan företag förbättra sin efterlevnad, stärka sina interna kontroller och minska risken för överträdelser inom kreditgivning och penningtvätt. Det är avgörande att prioritera höga standarder för efterlevnad och integritet för att säkerställa långsiktig stabilitet i företaget och förtroende inom finanssektorn.

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