Göteborgs Stad

Tjänsteutlåtande
Utfärdat 2026-09-09
Ärendenummer FGL-2026-00005

Handläggare
Petra Willquist Rönnäng
Telefon:
E-post: petra.willquist.ronnang@gotalejon.goteborg.se

Regelefterlevnadsfunktionens rapport kvartal 2 2026

Förslag till beslut

I styrelsen för Försäkrings AB Göta Lejon:

Styrelsen antecknar regelefterlevnadsfunktionens rapport kvartal 2 2026.

Sammanfattning

Regelefterlevnadsfunktionen avrapporterar den granskning som utförts i enlighet med beslutad granskningsplan. Funktionen för regelefterlevnad har vid fullgörandet av sitt uppdrag anmärkt på bolagets arbete med att säkerställa att alla IKT-avtal är på plats, men i övrigt 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

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

Bilagor som ingår i beslutsunderlaget

Regelefterlevnadsfunktionens kvartalsrapport 2 2026

Beskrivning av ärendet

Information till styrelsen om regelefterlevnadsfunktionens rapport från kvartal 2 2026.

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. Andra kvartalet har regelefterlevnadsfunktionen kontrollerat bolagets personuppgiftshantering i enlighet med dataskyddsförordningen, bolagetsinterna regler och riktlinjer för rapportering till Finansinspektionen, anpassning till nya eller förändrade regelverk samt övrig regelefterlevnad.

Regelefterlevnadsfunktionen har i samband med tidigare granskningar lämnat en rekommendation avseende att visst arbete kvarstår med att ta fram tilläggsavtal med IKT-leverantörer samt att vissa leverantörer uppvisat svårighet med att efterleva redan uppdaterade IKT-avtal. Denna rekommendation kvarstår och avses följas upp under tredje kvartalet.

Utförda kontroller har i övrigt 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.

Bolagets bedömning

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

Petra Willquist Rönnäng	Anders Jonasson
Bolagscontroller	VD

Till
Styrelsen i Försäkrings AB Göta Lejon

Kvartalsrapport för perioden 1 april 2026 – 30 juni 2026 avseende regelefterlevnad

1. Inledning

Genom denna rapport återkopplar funktionen för regelefterlevnad resultatet av senast genomförda kontroll av Försäkrings AB Göta Lejons, nedan Bolaget, regelefterlevnad samt redogör för de övriga åtgärder som funktionen för regelefterlevnad har vidtagit under det andra kvartalet 2026.

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 andra kvartal. Dessa finns återgivna i sin helhet i bilaga 2.

- Finansinspektionen ger Norion Bank AB en anmärkning och sanktionsavgift.
- Finansinspektionen ger Ikano Bank AB en anmärkning och sanktionsavgift.
- Årsrapport för 2025 om allvarliga IKT-relaterade incidenter.

2.2. Kontroll av Bolagets regelefterlevnad

Metod

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

Därtill har mer stickprovsbaserade kontroller utförts avseende rapportering, riktlinjer för riskhantering och återförsäkringsrisker. Gällande rapportering har funktionen för regelefterlevnad stämt av med Bolaget att relevant rapportering till Finansinspektionen har utförts.

Gällande granskning av rutiner och riktlinjer har dessa dels diskuterats vid kontrollmöte med Bolaget, dels granskats av funktionen för regelefterlevnad mot bakgrund av relevanta regelverk.

Relevanta regler och riktlinjer

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

- Försäkringsrörelselag (2010:2043)
- FFFS 2015:8 om Försäkringsrörelse
- Dataskyddsförordningen (GDPR)
- DORA-förordningen
- Riktlinjer för riskhantering
- Rutiner för hantering av återförsäkringsrisker

GDPR - kontroll

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

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

Bolaget har vidare informerat om att det har förevarit vissa avstämningar med dataskyddsombudet och Bolaget har vidare informerat dataskyddsombudet. Dataskyddsombudet har dock inte utfört någon direkt kontroll eller uppföljning gentemot Bolaget.

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

Rapportering - Kontroll

Granskning av Bolagets interna rutiner och riktlinjer för rapportering till Finansinspektionen.

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

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

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

Övrig regelefterlevnad - Kontroll

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

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

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

   Funktionen för regelefterlevnad har granskat relevanta riktlinjer. Därtill har Bolaget och funktionen diskuterat återförsäkringsprogrammet samt justeringar som skett däri under år 2025.

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

Anpassning till nya eller förändrade regelverk

Uppföljning och kontroll avseende Bolagets arbete kring förändringarna i Solvens II-direktivet.

Anpassningarna till omarbetningen av Solvens II-direktivet består primärt i bl.a. förändrade regler kring hållbarhet, primärt avseende scenarion i ORSA, uppdatering av vissa styrdokument m.m. De omarbetade reglerna börjar gälla år 2027, så funktionen för

regelefterlevnad bedömer att översyn av nuvarande riktlinjer och processer kan påbörjas under det tredje kvartalet.

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

Uppföljning av tidigare kontroller

Därtill har funktionen för regelefterlevnad följt upp tidigare rekommendationer avseende Bolagets arbete med IKT och informationssäkerhet.

Funktionen för regelefterlevnad har huvudsakligen inte haft några synpunkter med anledning av kontrollen, men noterar att vissa tilläggsavtal med IKT-leverantörer ännu inte är klara samt att vissa leverantörer uppvisat svårighet med att efterleva redan uppdaterade IKT-avtal.

Funktionen för regelefterlevnad har för avsikt att följa upp detta under det tredje kvartalet.

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

De oklarheter som funktionen för regelefterlevnad noterat framgår under avsnitt 2.2. ovan. Funktionen för regelefterlevnad har i övrigt 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 2 juli 2026

Johan Grenefalk

1 Översikt regelefterlevnad för kvartal 2, 2026

	Område	*Kontroll*	*Anmärkning*
	GDPR	Hantering av personuppgifter.	Ingen anmärkning.
	Rapportering	Rapportering till Finansinspektionen.	Ingen anmärkning.
	Övrig regelefterlevnad	Efterlevnad av regler för riskhantering.	Ingen anmärkning.
	Återförsäkring	Efterlevnad av reglerna om återförsäkringsrisker.	Ingen anmärkning.
	Anpassning till nya eller förändrade regelverk	Omarbetning av Solvens II-direktivet.	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*
	Q1 2026	Anpassning till nya eller förändrade regelverk (fokuskontroll)	Europaparlamentets och Rådets förordning om digital operativ motståndskraft för finanssektorn (DORA).	Visst arbete kvarstår alltjämt med Bolagets IKT-avtal, se notering i tillhörande kvartalsrapport, avsnitt 2.2.

*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.

Bilaga 2

Nyhetsbrev

Ang. Finansinspektionen ger Norion Bank AB en anmärkning och sanktionsavgift

---

28 maj 2026

1. Sammanfattning

Följande nyhetsbrev belyser Norion Bank AB:s, nedan Bolaget, efterlevnad av penningtvättsregelverket med särskilt fokus på kundkännedom. Finansinspektionen, nedan FI, har granskat hur Bolaget har arbetat med att hantera risker kopplade till penningtvätt och finansiering av terrorism.

FI har anfört att Bolaget i flera avseenden brustit i sin regelefterlevnad. Bolaget har inte vidtagit nödvändiga åtgärder för att bedöma om kunder, förknippade med medelhög eller hög risk för penningtvätt och finansiering av terrorism, haft verkliga huvudmän som varit personer i politiskt utsatt ställning (PEP) eller närstående till sådana personer (RCA). Bolaget har heller inte vidtagit skärpta kundkännedomsåtgärder för att inhämta information om högriskkunders affärsverksamhet eller ekonomiska situation och uppgifter om varifrån kundens ekonomiska medel kommer.

FI anser att överträdelserna inte är så allvarliga att det finns anledning att återkalla tillståndet, men tillräckligt allvarliga för att ge Bolaget en anmärkning förenad med en sanktionsavgift om 90 miljoner kronor.

2. Bakgrund

Bolaget, tidigare Collector Bank AB, har tillstånd att driva bankrörelse enligt lagen (2004:297) om bank- och finansieringsrörelse (LBF) och bedriver verksamhet inom verksamhetsområden och varumärken: Norion Bank, Walley och Collector. Bolaget erbjuder olika typer av krediter, såsom företags- och fastighetslån, samt inlåningskonton, till exempel sparkonton. Bolaget erbjuder även andra typer av finansiella tjänster och produkter som bland annat förvärv av fakturor (factoring) och betaltjänster.

Bolaget har såväl fysiska som juridiska personer som kunder. Under undersökningsperioden hade Bolaget cirka 11 000 företagskunder, varav ungefär en tredjedel tillhörde branscher förknippade med hög risk för penningtvätt och finansiering av terrorism. Bolaget är noterat på Nasdaq Stockholm och är moderföretag i en koncern med verksamhet i Sverige, Norge, Danmark, Finland och Tyskland.

,

3. Finansinspektionens ingripande

FI har i maj 2023 inlett en undersökning av Bolaget för att granska hur Bolaget under perioden den 30 april 2022 – 1 maj 2023 hade följt centrala bestämmelser i lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen). Undersökningen har fokuserat på vilka åtgärder för kundkännedom som Bolaget vidtagit avseende kunder som är juridiska personer. FI har granskat kundakter avseende 43 kunder som använt Bolagets inlåningskonton (sparkonton).

FI har identifierat två huvudsakliga brister.

3.1. Bristfälliga bedömningar av PEP och RCA

Vilka åtgärder som krävs för att bedöma om en kunds verkliga huvudman är PEP eller RCA styrs av den risk som kan förknippas med kundrelationen. Beroende på risknivån kan kontrollen i vissa fall fullgöras genom kontroll mot PEP- och RCA-listor, medan sådana åtgärder i andra fall inte är tillräckliga. Eftersom 41 av de granskade kunderna bedömts vara förknippade med medelhög eller hög risk har Bolaget varit skyldigt att vidta relativt omfattande kontrollåtgärder, särskilt avseende de 31 kunder som klassats som högrisk.

Av underlaget i ärendet framgår inte att Bolaget vidtagit några andra åtgärder än att fråga kunderna om deras verkliga huvudmän varit PEP eller RCA. Bolaget har visserligen hävdat att kontroller även gjorts mot PEP- och RCA-listor under undersökningsperioden, men FI har konstaterat att det underlag som Bolaget gett in inte ger stöd för detta påstående och att Bolaget inte lämnat någon godtagbar förklaring till varför sådant underlag saknas.

I detta avseende framhåller FI att en verksamhetsutövare är skyldig att i fem år bevara underlag som visar vilka kundkännedomsåtgärder som har vidtagits (5 kap. 3 § penningtvättslagen). Vid bedömningen av vilka åtgärder som faktiskt vidtagits är det därför rimligt att utgå från det som finns dokumenterat och kan kontrolleras. FI bedömer att avsaknaden av dokumentation speglar de verkliga förhållandena, dvs. att Bolaget inte genomfört några andra kontroller än att ställa frågor till kunderna.

Mot denna bakgrund kan Bolaget inte anses ha gjort en tillräcklig bedömning av om kundernas verkliga huvudmän varit PEP eller RCA, och har inte uppfyllt kraven i 3 kap. 10 § penningtvättslagen.

,

3.2. Bristfällig information om högriskkunder

Undersökningen har vidare visat att Bolaget bedömt att 32 av 43 inlåningskunder varit förknippade med hög risk för penningtvätt och finansiering av terrorism under hela eller åtminstone halva undersökningsperioden. Bolaget har under denna tid varit skyldigt att vidta skärpta kundkännedomsåtgärder för dessa kunder. FI framhåller att verksamhetsutövarens riskbedömning vid den aktuella tidpunkten är vägledande för vilka åtgärder som krävs, ju högre risk, desto mer omfattande åtgärder, och att Bolagets senare omvärdering och sänkning av riskklassen inte påverkar denna bedömning.

Skärpta åtgärder innebär enligt 3 kap. 16 § penningtvättslagen bland annat att inhämta ytterligare information om kundens affärsverksamhet, ekonomiska situation och varifrån kundens ekonomiska medel kommer. Av kundakterna framgår det att inga sådana åtgärder har vidtagits, vilket Bolaget medgett. FI konstaterar vidare att Bolagets transaktionsövervakning saknar relevans för bedömningen, eftersom övervakning av pågående affärsförbindelser utgör en annan del av arbetet med att förhindra penningtvätt och finansiering av terrorism och inte kan ersätta kundkännedomsåtgärder. Bolaget har därmed inte uppfyllt kraven i 3 kap. 16 § penningtvättslagen.

3.3. Val av ingripande och sanktionsavgift

Vid en sammantagen bedömning anser FI att överträdelserna inte är att bedöma som allvarliga i den mening som avses i 15 kap. 1 § tredje stycket LBF. Det är därmed inte aktuellt att återkalla Bolagets tillstånd eller att meddela Bolaget en varning. FI ger därför Bolaget en anmärkning som ska förenas med en sanktionsavgift för att vara tillräckligt ingripande.

4. HSA Söderqvist Advokatbyrås rekommendationer

Mot bakgrund av beslutet rekommenderar HSA Söderqvist Advokatbyrå att bolag som omfattas av reglerna om penningtvätt och finansiering av terrorism särskilt ska ta hänsyn till följande:

- Att enbart förlita sig på kundens egna uppgifter är inte tillräckligt vid medelhög eller hög risk. Det räcker inte att enbart fråga kunden om dennes verkliga huvudman är PEP eller RCA och sedan godta svaret utan vidare åtgärder. Vilka kontrollåtgärder som krävs styrs av den risk som kan förknippas med kundrelationen – ju högre risk, desto mer omfattande åtgärder. Vid medelhög eller hög risk bör kontrollen som utgångspunkt inkludera aktiv kontroll mot externa PEP- och RCA-listor.

,

- Se över riskklassificeringen och säkerställ att den återspeglar kundrelationens faktiska risk. En felaktig eller inaktuell riskklassificering får direkta konsekvenser för vilka kundkännedomsåtgärder som vidtas. Det bör säkerställas att riskklassificeringen uppdateras löpande och att förändringar i kundrelationen fångas upp och dokumenteras.

- En hög riskklass medför skyldighet att vidta skärpta kundkännedomsåtgärder. Det räcker inte att hålla en hög riskklass i systemet om detta inte omsätts i konkreta och dokumenterade åtgärder. Sådana åtgärder kan bland annat innebära att inhämta ytterligare information om kundens affärsverksamhet, ekonomiska situation och varifrån kundens medel kommer. FI är vidare tydlig med att transaktionsövervakning utgör en separat del av AML-arbetet och inte kan ersätta kundkännedomsåtgärder.

- Vidtagna åtgärder måste dokumenteras. En verksamhetsutövare är skyldig att bevara underlag som visar vilka kundkännedomsåtgärder som vidtagits. I en tillsynssituation gäller i praktiken att det som inte är dokumenterat inte kan anses ha genomförts. Det bör därför säkerställas att samtliga vidtagna åtgärder dokumenteras löpande och på ett verifierbart sätt.

- Tillsynstrycket ökar mot mindre och mellanstora finansiella aktörer. FI har konstaterat att kriminella i takt med att de större bankerna förbättrat sitt AML-arbete i stället söker sig till mindre aktörer. Bolag bör därför se över sitt AML-arbete proaktivt.

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

Nyhetsbrev

Ang. Finansinspektionen ger Ikano Bank AB en anmärkning och sanktionsavgift

---

17 juni 2026

1. Sammanfattning

Följande nyhetsbrev belyser Ikano Bank AB:s, nedan Bolaget, efterlevnad av penningtvättsregelverket, med särskilt fokus på den allmänna riskbedömningen och kundkännedom. Finansinspektionen, nedan FI, har granskat hur Bolaget har arbetat med att hantera risker kopplade till penningtvätt och finansiering av terrorism.

FI uppmärksammar att kriminella i ökad utsträckning söker sig till mindre och mellanstora banker i takt med att de större förbättrar sitt förebyggande arbete. Mot bakgrund av att Bolaget verkar inom banksektorn och har juridiska personer som kunder, vars komplexa ägar- och kontrollstrukturer kan försvåra identifiering av verkliga huvudmän, bedömer FI att risken för att verksamheten kan utnyttjas för penningtvätt och finansiering av terrorism är förhöjd.

FI har anfört att Bolaget i flera avseenden brustit i sin regelefterlevnad. Bolagets allmänna riskbedömning har bland annat saknat en verklighetsanpassad och fullständig bedömning av hur Bolagets företagsprodukter kan utnyttjas för finansiering av terrorism, samt hur stor risken är för detta. Vidare har Bolaget inte identifierat och beaktat riskfaktorer som är förknippade med dess faktiska kunder. Gällande kundkännedom har Bolaget inte vidtagit de skärpta kundkännedomsåtgärder som var nödvändiga i förhållande till kunder som var förknippade med hög risk för penningtvätt och finansiering av terrorism.

Enligt FI har överträdelserna inneburit en ökad risk för att Bolaget och det finansiella systemet kan utnyttjas för penningtvätt och finansiering av terrorism. FI ger därmed Bolaget en anmärkning och beslutar om en sanktionsavgift på 140 miljoner kronor.

2. Bakgrund

Bolaget har tillstånd att driva bankrörelse enligt lagen (2004:297) om bank- och finansieringsrörelse (LBF) och erbjuder bland annat krediter, inlåningskonton (sparkonton), fakturaköp och fakturabelåning (factoring) samt upplåter lös egendom (leasing). Bolagets verksamhet riktar sig till såväl fysiska som juridiska personer. Under undersökningsperioden hade Bolaget cirka 17 500 företagskunder som var juridiska personer.

,

Bolaget bedriver sin huvudsakliga verksamhet i Sverige men är även verksam i ett antal andra länder inom och utanför EES. Bolaget ingår i Ingka-koncernen och hade för räkenskapsåret 2025 en omsättning om cirka 7 220 miljoner kronor.

3. Finansinspektionens ingripande

FI inledde i maj 2023 en undersökning av Bolaget för att granska hur Bolaget under perioden den 30 april 2022 – 1 maj 2023 hade följt centrala bestämmelser i lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen). Undersökningen avgränsades till den verksamhet som riktar sig till kunder som är juridiska personer och fokuserade dels på Bolagets allmänna riskbedömning, dels på vilka åtgärder för kännedom som vidtagits. FI har granskat kundakter avseende 70 företagskunder med medelhög eller hög riskklass.

3.1. Brister i den allmänna riskbedömningen

Det framgår av 2 kap. 1 § första stycket penningtvättslagen att en verksamhetsutövare ska bedöma hur de produkter och tjänster som tillhandahålls i verksamheten kan utnyttjas för penningtvätt eller finansiering av terrorism samt hur stor risken är för att detta sker (allmän riskbedömning). Det följer vidare av 2 kap. 2 § första stycket penningtvättslagen att riskbedömningen ska vara verksamhetsanpassad och ligga till grund för verksamhetsutövarens rutiner, riktlinjer och övriga åtgärder mot penningtvätt och finansiering av terrorism.

Av utredningen framgår att Bolaget inte gjort någon verklighetsanpassad, separat och fullständig bedömning av hur de produkter som erbjuds företagskunder kan utnyttjas för finansiering av terrorism och hur stor risken är för detta. FI konstaterar även att Bolaget inte identifierat eller beaktat riskfaktorer som är förknippade med de kundtyper som Bolaget faktiskt har. Enligt FI omfattar detta bland annat kunder som använder Bolagets factoring- och leasingprodukter.

FI framhåller även att Bolaget inte beaktat information från myndigheter om risker och tillvägagångssätt för penningtvätt och finansiering av terrorism i den allmänna riskbedömningen. Bolaget hade enligt FI inte analyserat hur exempelvis insamlingsverksamhet, styrelsemålvakter och tillvägagångssätt vid skattebrott kan påverka den egna verksamheten.

Mot denna bakgrund bedömer FI att den allmänna riskbedömningen inte varit utformad på ett sådant sätt att den kunnat ligga till grund för Bolagets rutiner, riktlinjer och övriga

,

åtgärder mot penningtvätt och finansiering av terrorism. Bolaget anses därmed inte ha uppfyllt kraven i 2 kap. 1 § penningtvättslagen.

3.2. Otillräckliga skärpta kundkännedomsåtgärder

Undersökningen har vidare visat att Bolaget bedömt att 32 av de 70 granskade företagskunderna varit förknippade med hög risk för penningtvätt eller finansiering av terrorism under hela eller delar av undersökningsperioden. Bolaget har under denna tid varit skyldig att vidta skärpta kundkännedomsåtgärder för dessa kunder. FI framhåller att verksamhetsutövarens riskbedömning är vägledande för vilka åtgärder som krävs och att hög risk förutsätter mer omfattande kundkännedomsåtgärder.

Skärpta kundkännedomsåtgärder innebär enligt 3 kap. 16 § penningtvättslagen bland annat att inhämta ytterligare information om kundens affärsverksamhet, ekonomiska situation och varifrån kundens ekonomiska medel kommer. Av kundakterna framkommer att Bolaget i vissa fall endast inhämtat begränsad information om kundernas medel och att sådan information i andra fall har saknats helt.

Exempelvis hade en kund en verklig huvudman som var familjemedlem till en person i politiskt utsatt ställning och således bedömdes risker med kundrelationen som hög. Under undersökningsperioden genomförde kunden betalningar om drygt 20 miljoner kronor, trots det inhämtade Bolaget ingen information om varifrån kundens pengar kom.

En annan kund inom transport- och byggbranschen hyrde lastbil och kran via leasing. Ikano rapporterade kunden till Polismyndigheten med misstanke om penningtvätt och målvakter i styrelsen, men vidtog därefter inga ytterligare kundkännedomsåtgärder för att klarlägga varifrån kundens pengar kom.

FI bedömer att Bolaget därmed inte vidtagit de skärpta kundkännedomsåtgärder som krävts för att uppnå tillräcklig kundkännedom. Bolaget har således inte uppfyllt kraven i 3 kap. 16 § penningtvättslagen.

4. HSA Söderqvist Advokatbyrås rekommendationer

Mot bakgrund av beslutet rekommenderar HSA Söderqvist Advokatbyrå att bolag som omfattas av reglerna om penningtvätt och finansiering av terrorism särskilt ska ta hänsyn till följande:

- **Säkerställ att den allmänna riskbedömningen är verksamhetsanpassad och utformad så att den kan ligga till grund för verksamhetens rutiner, riktlinjer och övriga åtgärder mot penningtvätt och finansiering av terrorism.** Riskbedömningen bör utgå från

,

verksamhetens faktiska produkter, tjänster och kunder och distributionskanaler. Generella riskbeskrivningar är inte tillräckliga om de saknar koppling till verksamhetens faktiska risker. Det bör även säkerställas att identifierade risker får genomslag i verksamhetens fortsatta arbete.

- Att identifiera kundriskfaktorer som saknar koppling till kundbasen är inte tillräckligt. De riskfaktorer som beaktas i den allmänna riskbedömningen bör vara relevanta för de kunder som använder verksamhetens produkter och tjänster.

- Information från myndigheter om risker och tillvägagångssätt för penningtvätt och finansiering av terrorism bör inte enbart beaktas på övergripande nivå. Det bör säkerställas att sådan information analyseras utifrån den egna verksamheten och omsättas i den allmänna riskbedömningen.

- Om risken med en kundrelation bedöms som hög medför det en skyldighet att vidta skärpta kundkännedomsåtgärder. Det är inte tillräckligt att klassificera en kund som högriskkund om inte detta inte följs av åtgärder. Sådana åtgärder kan bland annat innebära att inhämta information om kundens affärsverksamhet, ekonomiska situation och varifrån kundens ekonomiska medel kommer.

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

Nyhetsbrev

Ang. årsrapport för 2025 om allvarliga IKT-relaterade incidenter

25 juni 2025

1. Bakgrund

Genom DORA har ett harmoniserat ramverk introducerats för finansiella entiteters hantering, klassificering och rapportering av IKT-relaterade incidenter. Syftet är att säkerställa att allvarliga incidenter anmäls till samtliga berörda behöriga myndigheter på ett enhetligt sätt, vilket möjliggör ett snabbare och mer samordnat agerande vid gränsöverskridande händelser.

De tre europeiska tillsynsmyndigheterna EBA, ESMA och EIOPA, nedan ESA, ska årligen rapportera om allvarliga IKT-relaterade incidenter. Rapporten ska som minst redovisa antalet incidenter, deras karaktär, påverkan på finansiella entiteters verksamhet och kunder, vidtagna åtgärder samt uppkomna kostnader. Nedan följer vilka centrala mönster och trender ESA noterat efter att ha analyserat rapporterade allvarliga IKT-relaterade incidenter under år 2025.

2. Analys

Rapporten grundar sig på totalt 3 383 allvarliga incidenter som rapporterats av finansiella entiteter inom EU. Ungefär en tredjedel av dessa incidenter hade gränsöverskridande påverkan, vilket tydliggör den ökande sammankopplingen genom delade infrastrukturer och tjänster.

När det gäller incidenttyp rapporterades systemfel för 51 procent av alla större incidenter, följt av externa händelser, 27 procent, och betalningsrelaterade incidenter, 18 procent. Nästan en tredjedel av de större incidenterna härrörde från ett fel hos en tredjepartsleverantör. Detta understryker behovet av en robust hantering av tredjepartsrisker, effektiv tillsyn över utkontrakterade tjänster samt nära samordning med tjänsteleverantörer under incident- och återställningsarbetet.

Majoriteten av incidenterna har klassificerats som större främst på grund av varaktighet och tjänsteavbrott eller påverkan på kunder, finansiella motparter och transaktioner. Cirka 16 procent har klassificerats som större på grund av anseendepåverkan, exempelvis

,

medieuppmärksamhet, upprepade kundklagomål, risk för bristande regelefterlevnad eller väsentlig kundförlust.

Endast tio procent av incidenterna hade koppling till cybersäkerhet. Detta ska enligt ESA inte tolkas som att hotbilden är låg. Tvärtom ställer den snabba utvecklingen av avancerade AI-drivna verktyg ökade krav på finansiella entiteters förmåga att upprätthålla högsta möjliga cybersäkerhetsstandard. Försäkringsföretag är särskilt utsatta för ransomwareattacker. Detta kan förklaras av att försäkringsföretag innehar stora mängder känsliga hälso- och finansiella uppgifter.

Rapporten visar att påverkan på kunder, transaktioner och finansiella motparter har varit begränsad, trots incidenternas frekvens och i vissa fall breda geografiska räckvidd. Två tredjedelar av de större incidenterna har lett till ingen eller endast mindre störning för kunder och transaktioner, vilket tyder på att snabb upptäckt, i kombination med effektiva åtgärder för incidenthantering och begränsning, ofta lyckats begränsa operativ skada och spridningseffekter.

Sammantaget illustrerar rapporten den växande systemdimensionen av IKT-risk och vikten av att finanssektorn kontinuerligt stärker sin förmåga att förebygga, absorbera och återhämta sig från framtida incidenter.

3. HSA Söderqvist Advokatbyrås rekommendationer

Finansiella entiteter som omfattas av DORA bör ta fasta på de slutsatser som ESA presenterar i rapporten och använda dem som utgångspunkt för en löpande översyn av den egna IKT-riskhanteringen. Advokatbyråns bedömning är att särskild uppmärksamhet bör riktas mot tre områden.

Det första är tredjepartshantering. Avtalsstrukturer med IKT-leverantörer bör ses över i ljuset av DORA:s krav, och entiteter bör säkerställa att det finns etablerade eskaleringsvägar och samordningsrutiner som aktiveras vid en incident. Det andra är klassificering och rapportering. Interna processer för att identifiera, klassificera och anmäla allvarliga incidenter behöver vara tydliga och testade, så att rapporteringsskyldigheterna kan uppfyllas inom de tidsfrister som förordningen föreskriver. Det tredje är cybersäkerhetsförmåga. Med hänsyn till oro kring AI-drivna hot bör entiteter genomföra en bedömning av om befintliga säkerhetsåtgärder är tillräckliga och ändamålsenliga.

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