Till
Styrelsen i S:t Erik Försäkrings AB

Rapport för perioden 13 maj 2026 – 10 september 2026 avseende regelefterlevnad

1. Inledning

Genom denna rapport redovisar funktionen för regelefterlevnad resultatet av senast genomförda kontroll av S:t Erik Försäkrings AB:s, nedan Bolaget, regelefterlevnad samt redogör för de övriga åtgärder som funktionen har vidtagit under perioden.

2. Händelser av relevans under perioden

2.1. Regelbevakning och relevanta sanktionsbeslut

Under perioden har följande nyhetsbrev tillställts Bolaget. Dessa återfinns i sin helhet i bilaga 1.

- 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
- Nya nationella råd och rekommendationer om cybersäkerhetshot från avancerad AI
- Förslag om elektroniska meddelanden vid försäkringsavtal (Ds 2026:7)
- IMY klargör ansvarsroller enligt GDPR vid finjustering av AI

2.2. Kontroll av Bolagets regelefterlevnad

Kontroll av Bolagets regelefterlevnad har ägt rum genom ett möte med representanter från Bolaget samt genom granskning av handlingar.

Kontrollen utgår från den årsplan som funktionen för regelefterlevnad har upprättat inför verksamhetsåret och redogörs för närmare nedan.

Område	*Kontroll*	*Compliancerisk (Grön/Gul/Röd)*
Övrig regelefterlevnad	Intressekonflikter.	Kontrollen har inte föranlett några synpunkter.
	Kompetens och kunskapsnivå hos anställda (FDL/IDD).	Kontrollen har inte föranlett några synpunkter.
	Kompetens och kunskapsnivå hos styrelsen (fit & proper) inkl. samlad kompetens.	Kontrollen har inte föranlett några synpunkter.
Uppföljning föregående kvartal	DORA-förordningen	Bolaget har mottagit ett antal rekommendationer från funktionen för internrevision beträffande justeringar i styrdokument m.m. Bolaget och funktionen för regelefterlevnad delar uppfattningen att vissa saker kan förtydligas och kommer att arbeta med detta under år 2026.

Metod

Periodens 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.

Funktionen för regelefterlevnad har vidare följt upp den tidigare anmärkningen beträffande Bolagets hantering av anmärkningar från funktionen för internrevision beträffande justeringar i styrdokument m.m. kopplade till DORA-förordningen.

Relevanta regler och riktlinjer

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

- Försäkringsrörelselag (2010:2043)
- FFFS 2015:8 om Försäkringsrörelse

- Kommissionens delegerade förordning 2015/35 om upptagande och utövande av försäkringsverksamhet
- Riktlinjer för intressekonflikter
- Riktlinjer för kunskap och kompetens (fit & proper)
- Riktlinjer för försäkringsdistribution

Intressekonflikter - kontroll

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 styrelse. Utöver att det finns en anmälningsskyldighet avseende intressekonflikter i verksamheten så är det även en stående punkt vid varje styrelsesammanträde i Bolaget.

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

Kunskap och kompetens hos anställda - kontroll

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 ska avlägga kunskapstest avseende år 2026 den 28 september i år.

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-kontroll

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 2026 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 genomfördes i maj 2026.

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.

2.4. Styrelsesammanträde

Funktionen för regelefterlevnad har den 13 mars 2026 deltagit vid styrelsemöte i Bolaget och därvid redogjort för bl.a. föregående års årsrapport.

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 8 september 2026

Johan Grenefalk

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.

Nyhetsbrev

Ang. Nya nationella råd och rekommendationer om cybersäkerhetshot från avancerad AI

---

2 juli 2026

1. Bakgrund

AI förändrar sällan vilka typer av cyberangrepp som förekommer. Nationellt cybersäkerhetscenter, nedan NCSC, bedömer att AI främst kommer att förstärka befintliga angreppsmetoder, snarare än att skapa helt nya. När organisationer använder AI uppstår en ny cyberattackyta eftersom systemen är kontextberoende och tolkar input. Det gör dem sårbara för angrepp, särskilt när de kopplas till interna system, får tillgång till verksamhetsdata eller får möjlighet att agera autonomt. Grundläggande cybersäkerhetsprinciper gäller därför fortsatt, men de måste fungera bättre än någonsin och kompletteras med flexibilitet att utveckla nya förmågor. Insatser som begränsar angriparens möjligheter och ökar motståndskraften i verksamhetens system bör därför prioriteras.

2. Rekommendationer för beslutsfattare och organisationer

NCSC rekommenderar att cyberrisker hanteras som en ledningsfråga. Det innebär bl.a. att en verksamhet behöver ha ett tydligt ägarskap för system, informationstillgångar och AI-lösningar. Bristande underhåll, gamla och icke uppdaterade system samt oklart systemägarskap kan medföra affärsrisker med direkta konsekvenser för verksamhetens kontinuitet.

Verksamheten behöver även hålla hot- och riskanalyser uppdaterade utifrån såväl AI-förstärkta angrepp som risker kopplade till den egna användningen av AI. Det bör även finnas tillräckliga resurser och reservkapacitet för att leveranser ska kunna upprätthållas och att personal inte överbelastas.

NCSC lyfter även behovet av tydlig styrning av AI-användningen. Organisationer bör besluta vilka AI-verktyg som får användas, vilken information verktygen får hantera och när mänskligt godkännande krävs. Detta är särskilt viktigt eftersom avsaknad av beslut och policy ökar risken för skugg-IT.

,

Vid upphandling bör säkerhetskrav ställas, kontinuitets- och utträdesplaner säkras och efterlevnaden följas upp. Beredskapen kan därutöver stärkas genom samverkan i kunskapshöjande nätverk samt övningar som omfattar AI-förstärkta angrepp och manipulation.

3. Tekniska rekommendationer

På den tekniska sidan betonar NCSC att grundläggande cyberhygien fortsatt är avgörande och att den bör etableras genom NCSC:s tio rekommenderade säkerhetsåtgärder. Ju mer avancerade och AI-drivna hoten blir, desto viktigare blir grunderna, eftersom många avancerade angrepp bygger vidare på kända metoder.

AI kan förkorta tiden från att en sårbarhet blir känd till att den utnyttjas och därmed även tiden för att hinna åtgärda sårbarheten. Särskild prioritet bör därför ges till internetexponerade och affärskritiska system. Den internetexponerade attackytan bör samtidigt minska. Ju färre tjänster och system som är exponerade mot internet, desto färre vägar finns det att utnyttja.

Säkerhet bör även byggas in genom hela AI-systemets livscykel, från design och utveckling till drift och avveckling. I grunden är detta samma principer som gäller för övrigt, men AI tillför nya angreppsytor. Agentiska system bör begränsas eftersom de kan agera självständigt och därmed medföra risker. Systemen bör inte få tillgång till mer data än vad som faktiskt behövs. Tydliga behörighetsgränser bör sättas och mänsklig bekräftelse krävas innan känsliga eller irreversibla åtgärder utförs. Agentsystem med bred åtkomst och svag tillsyn utgör ett betydande riskscenario.

AI gör phising, röstkloning och falska dokument mer trovärdiga, vilket innebär att tidigare varningstecken inte längre är tillräckliga. NCSC rekommenderar därför löpande utbildning med realistiska och tydliga exempel. Organisationer bör kartlägga kritiska leverantörer och komponenter samt bevaka kända sårbarheter.

HSA Söderqvist Advokatbyrås rekommendationer

Mot bakgrund av NCSC bedömningar rekommenderar HSA Söderqvist Advokatbyrå att organisationer prioriterar följande åtgärder.

- Säkerställ styrning och ansvar. Cyberrisker och användningen av AI bör hanteras på ledningsnivå. Fastställ ett tydligt ansvar för verksamhetens system, informationstillgångar och AI-lösningar, och säkerställ att hot- och riskanalyser som omfattar både AI-förstärkta angrepp och risker kopplade till den egna användningen

,

av AI är säkrade. Upprätta därtill skriftliga styrdokument för användandet av AI-verktyg där användandet och den uppföljande kontrollen, tydligt regleras.

- Inför en tydlig och kontrollerad AI-användning. Fastställ vilka AI-verktyg som får användas, vilken information som får delas med dem och i vilka situationer mänskligt godkännande krävs. Särskild försiktighet bör iakttas när AI-system får tillgång till interna system, verksamhetsdata eller möjligheten att agera självständigt.
- Prioritera de grundläggande skyddsåtgärderna. Säkerställ skyndsam uppdatering av internetexponerade och affärskritiska system samt löpande kontroller av den internetexponerade attackytan. Begränsa samtidigt behörigheter och åtkomst till vad som är nödvändigt, särskilt för agentiska system.
- Stärkt beredskap i hela verksamheten. Säkerställ återkommande utbildning och som omfattar AI-förstärkta angrepp. Ställ även tydliga säkerhetskrav på leverantörer, följ upp kritiska externa komponenter och bevaka kända sårbarheter i leverantörskedjan.

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

Nyhetsbrev

Ang. Förslag om elektroniska meddelanden vid försäkringsavtal (Ds 2026:7)

---

21 augusti 2026

1. Sammanfattning

Detta nyhetsbrev belyser promemorian ”Elektroniska meddelanden vid försäkringsavtal (Ds 2026:7)”, som överlämnats till Justitiedepartementet efter en särskild utredning om formkraven i försäkringsavtalslagen (2005:104), nedan FAL. Bakgrunden är att FAL innehåller varierande och delvis oklara krav på hur meddelanden från försäkringsbolag till försäkringstagare ska utformas, vilket den ökade digitaliseringen av försäkringsverksamheten aktualiserar.

Förslaget innebär att en ny bestämmelse om formkrav för vissa meddelanden från försäkringsbolaget införs i 1 kap. 9 § FAL. Enligt förslaget ska sådana meddelanden från försäkringsbolag som påverkar rättigheter eller förpliktelser enligt ett gällande avtal om individuell försäkring, så kallade påbud (till exempel uppsägning, hävning eller villkorsändring). Sådana meddelanden ska kunna sändas med post eller elektroniskt, förutsatt att försäkringstagaren omedelbart kan ta del av dem. Motsvarande ska gälla vid gruppförsäkring när ett meddelande med sådan verkan ska sändas till en gruppmedlem personligen. Ren information och påminnelser omfattas inte av den nya regeln så FAL:s och lagen (2018:1219) om försäkringsdistributions, nedan LFD, befintliga informationsregler lämnas oförändrade.

Vidare föreslås att ett förmånstagarförordnande, liksom återkallelse eller ändring av ett sådant, ska kunna göras genom ett elektroniskt meddelande som undertecknas med avancerad elektronisk underskrift enligt eIDAS-förordningen, som ett alternativ till dagens krav på egenhändigt undertecknande i pappersform.

De föreslagna reglerna föreslås träda i kraft den 1 juli 2027 och ska som utgångspunkt inte gälla för avtal som ingåtts före ikraftträdandet och som inte förnyats därefter. Förslaget har skickats på remiss till berörda remissinstanser och svar ska lämnas senast den 28 augusti 2026.

,

2. Förslaget och skälen för det

Den föreslagna huvudregeln innebär att meddelanden som utgör påbud, det vill säga rättshandlingar som medför rättsverkningar för mottagaren (till exempel uppsägning, hävning, preskriptionsavbrott eller villkorsändring), ska skickas med post eller elektroniskt så att försäkringstagaren omedelbart kan ta del av dem. Det ska gälla oavsett om FAL eller annan författning föreskriver en viss form, till exempel skriftlighet. Det räcker dock inte att enbart hänvisa till en webbplats eller till försäkringstagarens "Mina sidor", eftersom en sådan ordning inte säkerställer att försäkringstagaren omedelbart uppmärksammar meddelandet och kan vidta åtgärder för att bevara sitt skydd.

Utredningen har övervägt men avstått från att låta försäkringstagare vid konsument- och personförsäkring välja kommunikationssätt, med motiveringen att andelen försäkringstagare som har svårt att hantera elektronisk kommunikation minskar och att branschen redan i praktiken anpassar sig efter försäkringstagarens behov. Regeln föreslås vara tvingande i den delen som avser att försäkringstagaren omedelbart ska kunna ta del av meddelandet, men parterna kan avtala om huruvida kommunikationen ska ske per post eller elektroniskt.

När det gäller förmånstagarförordnanden föreslås ett tillägg till 14 kap. 3 § FAL som, utöver dagens krav på egenhändigt undertecknat meddelande i pappersform, tillåter elektroniskt undertecknande med avancerad elektronisk underskrift enligt artikel 3 i eIDAS-förordningen. Förslaget svarar mot ett önskemål som Svensk Försäkring framställt och bedöms inte medföra minskad rättssäkerhet jämfört med egenhändigt undertecknande.

3. Dataskydd

Förslaget innebär att försäkringsbolagen ska behandla personuppgifter i syfte att kommunicera med försäkringstagare i avtalsfrågor, vilket i allt väsentligt rör uppgifter som bolagen redan behandlar idag. Den rättsliga grunden för behandlingen är i första hand att den är nödvändig för att fullgöra avtalet med försäkringstagaren enligt artikel 6.1 b i dataskyddsförordningen. Förslaget bedöms inte medföra några betydande förändringar av försäkringsbolagens nuvarande personuppgiftsbehandling eller innebära ett ökat intrång i den personliga integriteten.

Förslaget bedöms dock kunna begränsas till personuppgifter som inte utgör känsliga personuppgifter. Det bör typiskt sett inte finnas anledning att låta ett elektroniskt påbud till försäkringstagaren innehålla sådana uppgifter. Om det i ett enskilt fall är nödvändigt att behandla känsliga personuppgifter krävs stöd enligt artikel 9.2 i dataskyddsförordningen.

,

4. HSA Söderqvist Advokatbyrås rekommendationer

Mot bakgrund av förslaget rekommenderar HSA Söderqvist Advokatbyrå att försäkringsbolagen fortsätter att sända påbud, såsom uppsägning, hävning och villkorsändring, direkt till försäkringstagaren, till exempel per post eller via e-post, så att försäkringstagaren omedelbart kan ta del av meddelandet. Försäkringsbolagen ska inte enbart hänvisa till en webbplats eller kundportal för denna typ av meddelanden. Ren information och påminnelser omfattas inte av den föreslagna regeln. För dessa meddelanden gäller även fortsättningsvis de informations- och formkrav som följer av FAL och LFD. Försäkringsbolagen bör även säkerställa att elektroniska påbud inte innehåller känsliga personuppgifter utan särskilt stöd i artikel 9.2 i dataskyddsförordningen.

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

Nyhetsbrev

Ang. IMY klargör ansvarsroller enligt GDPR vid finjustering av AI

---

28 augusti 2026

1. Bakgrund

AI har på kort tid blivit en central del av många verksamheters digitala utveckling. Samtidigt har frågor om dataskydd och ansvarsfördelning blivit alltmer aktuella, särskilt när AI-modeller anpassas eller finjusteras med hjälp av data som kan innehålla personuppgifter. För att ge vägledning på området har Integritetsskyddsmyndigheten, nedan IMY, publicerat en rapport som analyserar vilka roller olika aktörer kan ha enligt GDPR vid finjustering av AI-applikationer. Rapporten har tagits fram inom ramen för IMY:s regulatoriska sandlåda och syftar till att skapa större tydlighet för både leverantörer och användare av AI-tjänster.

2. Den faktiska behandlingen avgör ansvaret

Ett av rapportens viktigaste budskap är att ansvarsfördelningen enligt GDPR inte avgörs av vilken teknik som används eller vad parterna väljer att kalla sig i ett avtal. Istället är det den faktiska behandlingen av personuppgifter som är avgörande. Bedömningen måste utgå från vem som bestämmer varför personuppgifter behandlas och vilka väsentliga beslut som fattas kring behandlingen. Detta innebär att organisationer behöver göra en korrekt analys av varje behandlingsaktivitet i ett AI-projekt och inte enbart förlita sig på generella antaganden om roller och ansvar.

2.1. När leverantören är personuppgiftsansvarig

IMY konstaterar att en AI-leverantör ofta blir personuppgiftsansvarig när denne använder personuppgifter för att utveckla eller förbättra sina egna produkter och tjänster. Om leverantören exempelvis finjusterar sin AI-modell för att förbättra dess prestanda eller utveckla nya funktioner för framtida kunder är det leverantören som bestämmer ändamålet med behandlingen. I sådana situationer ansvarar leverantören för att det finns en giltig rättlig grund för behandlingen och att samtliga krav enligt GDPR uppfylls.

För många organisationer innebär detta att användningen av kunddata för egen produktionsutveckling kräver en mer genomtänkt dataskyddsanalys än vad som tidigare varit fallet.

,

2.2. När leverantören agerar som personuppgiftsbiträde

I andra situationer sker behandlingen enbart på uppdrag av kunden. Om en AI-modell finjusteras för en specifik kunds verksamhet och kunden bestämmer både syftet med behandlingen och vilka uppgifter som ska användas, är det normalt kunden som är personuppgiftsansvarig. Leverantören agerar då som personuppgiftsbiträde och får endast behandla uppgifterna enligt kundens dokumenterade instruktioner.

Rapporten understryker vikten av att ansvarsfördelningen tydligt regleras genom personuppgiftsbiträdesavtal och att det finns en gemensam förståelse för vilka instruktioner som gäller under hela utvecklings- och förvaltningsprocessen.

2.3. När gemensamt personuppgiftsansvar uppstår

IMY lyfter även fram att det finns situationer där varken kunden eller leverantören ensamma bestämmer över behandlingen. I gemensamma utvecklingsprojekt eller innovationssamarbeten kan båda parter påverka såväl syftet med behandlingen som de viktigaste besluten kring hur den ska genomföras. Då kan ett gemensamt personuppgiftsansvar uppstå. Enbart det förhållandet att parterna samarbetar eller har ett gemensamt ekonomiskt intresse är dock inte tillräckligt.

Ett sådant ansvar innebär att parterna tillsammans måste komma överens om hur GDPR-skyldigheterna ska fördelas och säkerställa att de registrerade får tydlig information om vem som ansvarar för vad.

2.4. Konsekvenser för organisationer som använder AI

En viktig slutsats i rapporten är att samma aktör kan ha olika roller i olika delar av samma AI-projekt. En leverantör kan exempelvis vara personuppgiftsbiträde när en kundanpassad modell utvecklas, men samtidigt vara personuppgiftsansvarig när data används för att förbättra den egna tjänsten. Detta innebär att ansvarsfördelningen måste analyseras löpande och dokumenteras på ett strukturerat sätt.

Mot denna bakgrund rekommenderar HSA Söderqvist Advokatbyrå att dataskyddsfrågorna beaktas redan vid utveckling och upphandling av AI-lösningar.

3. HSA Söderqvist Advokatbyrås rekommendationer

Mot bakgrund av IMY:s vägledning bör personuppgiftsansvariga genomföra en noggrann kartläggning av alla behandlingsaktiviteter som förekommer i samband med AI-utveckling, finjustering och användning. Det är viktigt att redan i planeringsfasen identifiera vilka

,

personuppgifter som behandlas, vilka aktörer som är involverade och vilka syften behandlingen ska uppfylla. Det räcker inte med att avtalsmässigt kalla sig för exempelvis personuppgiftsbiträde, eftersom det är den faktiska kontrollen över syfte och användning av personuppgifter som avgör rollen enligt GDPR.

Härtill bör personuppgiftsansvariga redan från början tydligt definiera ansvarsfördelningen mellan kund och leverantör, särskilt vid finjustering av AI-modeller och projekt där flera parter bidrar till utvecklingen av AI-lösningar, eftersom dessa situationer ofta innebär mer komplexa avtalsförhållanden.

Slutligen bör dataskyddsfrågorna integreras i organisationens övergripande AI-styrning. Genom att kombinera juridisk och teknisk kompetens kan organisationer skapa förutsättningar för en ansvarsfull användning av AI som både främjar innovation och säkerställer efterlevnad av GDPR.

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