Tjänsteutlåtande
Utfärdat 2025-11-06
Ärendenummer FGL-2024-00141

Handläggare
Petra Willquist Rönnäng
Telefon: 031-368 5514
E-post: petra.willquist.ronnang@gotalejon.goteborg.se

Regelefterlevnadsfunktionens rapport kvartal 3 2025

Förslag till beslut

I styrelsen för Försäkrings AB Göta Lejon:

Styrelsen antecknar regelefterlevnadsfunktionens rapport kvartal 3 2025.

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 arbeta utefter de dokumenterade processerna för avtalsuppföljning och leverantörskontroll, samt 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 3 2025

Beskrivning av ärendet

Information till styrelsen om regelefterlevnadsfunktionens rapport från kvartal 3 2025.

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. Tredje kvartalets kontroll har till övervägande del bestått i att följa upp bolagets anpassning till DORA-förordningen. Vidare har kontrollen innefattat uppföljning och kontroll avseende intressekonflikter, kunskap och kompetens hos anställda samt fit and proper.

Under kvartal 3 2025 har regelefterlevnadsfunktionen följt upp anmärkningen om att arbeta utefter de dokumenterade processerna för avtalsuppföljning och leverantörskontroll, samt säkerställa att alla IKT-avtal är på plats med de justeringar som behövs och kommer fortsätta göra detta.

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 juli - 30 september 2025 avseende regelefterlevnad

1. Inledning

Genom denna rapport återkopplar funktionen för regelefterlevnad resultatet av senast genomförd kontroll av Försäkrings AB Göta Lejons, nedan Bolaget, regelefterlevnad samt redogör för de övriga åtgärder som funktionen för regelefterlevnad har vidtagit under det tredje kvartalet 2025.

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

2. Händelser av relevans under perioden

2.1. Regelbevakning

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

- ESMA:s principer för myndigheters tillsyn av tredjepartsrisker (250704)
- Guide avseende tillsyn av tredjepartsleverantörer enligt DORA (250925)

2.2. Kontroll av Bolagets regelefterlevnad

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 från 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 anpassningar 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

Uppföljning av identifiering och hantering av intressekonflikter har gjorts. Kontrollen har syftat till att följa upp om Bolaget har identifierat några nya intressekonflikter som behövt hanteras.

Bolaget har redogjort för Bolagets interna rutiner för att identifiera och hantera intressekonflikter. Funktionen för regelefterlevnad har vidare tagit del av Bolagets interna riktlinjer för hantering av intressekonflikter som omfattar samtliga anställda och Bolagets ledning. Utöver att det finns en anmälningsskyldighet avseende intressekonflikter i verksamheten så är det även en stående punkt vid varje styrelsesammanträde i Bolaget. Funktionen har därtill utfört en särskild kontroll där anställda och styrelsen har fått besvara frågor angående intressekonflikter, samt intygat att inga sådana som kan påverka Bolaget negativt föreligger.

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

Kunskap och kompetens hos anställda

Granskning av Bolagets interna rutiner och riktlinjer för kunskap och kompetens. Kontrollen har syftat till att säkerställa att Bolaget har vidtagit rimliga åtgärder för att efterleva kunskaps- och fortbildningskravet i försäkringsdistributionsregelverket (IDD).

Bolaget har redogjort för sina 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 därtill avlägga kunskapstest den 23 oktober avseende år 2025.

Funktionen för regelefterlevnad bedömer sammantaget att Bolaget har goda rutiner och riktlinjer för att säkerställa efterlevnad av kraven på kunskap och kompetens enligt IDD.

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

Fit & proper

Uppföljning av styrelsens samlade kompetens. Kontrollen har syftat till att säkerställa att Bolagets styrelse efterlever kraven som ställs i Solvens II-regelverket på styrelsens samlade kompetens, samt följa upp om det finns behov av kompetensutveckling.

Bolagets styrelse har under år 2024 genomfört den årliga ”fit & proper”-övningen där samtliga styrelseledamöter skattat dels sin egen enskilda kunskap och kompetens, dels styrelsens samlade kompetens. I denna övning identifieras eventuella behov av kompetensutveckling och att Bolaget följer upp och justerar styrelsens utbildningsplan för kommande år. Under oktober kommer årets fit & proper att genomgås och fastställas av styrelsen.

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

Uppföljning från andra kvartalet

Funktionen för regelefterlevnad har under perioden följt upp Bolagets anpassningar till DORA-förordningen mot bakgrund av en tidigare anmärkning. Bolaget arbetar fortsatt med att få samtliga IKT-avtal på plats och funktionen kommer fortsatt följa upp detta arbete under det fjärde kvartalet av 2025.

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 anmärkningar funktionen för regelefterlevnad haft återges i avsnitt 2.2 ovan. I övrigt har funktionen för regelefterlevnad 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 10 oktober 2025

Johan Grenefalk

1 Översikt regelefterlevnad för kvartal 3, 2025

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

*Denna matris syftar till att ge Bolaget en överblick över resultatet av utförd kontroll av Bolagets regelefterlevnad samt återge vilka åtgärder som Bolaget rekommenderas att vidta eller som är under arbete. Denna färgskala är inte kopplad till den riskmatris som har tillsänts Bolaget som bilaga till årsplanen.

2 Översikt regelefterlevnad från föregående kontroller

	Kvartal	*Område*	*Kontroll*	*Anmärkning*
	Q2 2025	Anpassning till nya eller förändrade regelverk (fokuskontroll)	Europaparlamentets och rådets förordning om digital operativ motståndskraft för finanssektorn (DORA).	*Se kommentar i avsnitt 2.2 i kvartalsrapporten för det andra kvartalet.*

*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.

Nyhetsbrev

4 juli 2025

Ang. ESMA:s principer för myndigheters tillsyn av tredjepartsrisker

---

1. Bakgrund

Europeiska värdepappers- och marknadsmyndigheten, nedan ESMA, har under juni 2025 publicerat principer för tillsyn av tredjepartsrisker. Majoriteten av finansiella aktörer inom Europeiska unionens, nedan EU, värdepappersmarknadssektorer är beroende av tredjepartsleverantörer för att kunna tillhandahålla specifika tjänster. Traditionellt sett har dessa tjänster tillhandahållits genom utkontraktering. Digitaliseringen har däremot ökat detta beroende och kräver således ett utvidgat tillsynsperspektiv. Användning av tredjepartstjänster kan bidra till förbättrad service, expertis och kostnadsbesparingar. Däremot tillkommer även risker såsom förlust av kontroll, bristande efterlevnad, minskad operativ motståndskraft och koncentrationsrisker.

Principerna har införlivats för att hantera de risker som har observerats när finansiella aktörer använder sig av outsourcing, delegering eller andra former av tredjepartstjänster. Principerna erbjuder en gemensam tillsynsbas för nationella behöriga myndigheter och ESMA, ökar tillsynsramarnas robusthet och hjälper de finansiella aktörerna att förstå och hantera tredjepartsrisker. Principerna avser att stödja en gemensam och effektiv tillsyn inom EU. Principerna riktar sig till både tillsynsmyndigheter som ansvarar för att övervaka och reglera aktörer på EU:s finansmarknader, samt finansiella aktörer som står under dessa myndigheters tillsyn. Finansinspektionen är behörig tillsynsmyndighet i Sverige och har ännu inte uttalat sig om detta.

ESMA:s principer är icke-bindande och gäller för alla finansiella aktörer inom EU:s värdepappersmarknader som faller inom ESMA:s tillsynsmandat.

Det bör noteras att ESMA:s principer för tillsyn av tredjepartsrisker inte omfattar IKT-relaterade tredjepartsrisker, eftersom dessa regleras särskilt i DORA-förordningen.

2. Principer

2.1. Princip om tillsynsöversikt

Finansiella aktörer ansvarar för användning av tredjepartsleverantörers tjänster. Även om ansvaret för användning av tredjepartsleverantörer ligger hos den finansiella aktör som står under tillsyn, bör tillsynsmyndigheterna effektivt övervaka finansiella aktörers exponering för tredjepartsrisker. Tillsynsmyndigheterna har i uppdrag att säkerställa att ansvaret inte påverkar tillsynens kvalitet. Tillsynsmyndigheterna ska främja lämpliga styrnings- och riskramverk hos finansiella aktörer. Bedömning av tredjepartsrisker bör utföras genom auktorisation eller notifiering av nya eller

ändrade arrangemang. Tillsynsmyndigheterna ska inkludera risker i sina metoder för tillsyn, inklusive platsbesök och skrivbordgranskning. Tillsynsmyndigheterna bär även ett ansvar att vidta åtgärder vid eventuell oro avseende finansiella aktörers användning av tredjepartleverantörers tjänster och ska hantera samt identifiera eventuella koncentrationsrisker.

2.2. Principer för finansiella aktörer

Finansiella aktörer ska implementera effektiv styrning för att hantera tredjepartsrisker. Tredjepartsanvändning får inte äventyra självständigt beslutsfattande eller styrning. Styrelse och ledning får inte delegera tillsyns-, styrnings- eller beslutsansvar. Delegering av nyckelfunktioner såsom ansvarsområden inom förvaltning anses oförenligt med god styrning.

Ledningsorgan är ansvariga för övervakningen av tredjepartsrisker och ska besitta lämpliga kompetenser för att förstå och övervaka de risker som är kopplade till den verksamhet som tillhandahålls av tredjepartsleverantörer. ESMA anför att ledningsorgan bör utse en ansvarig person inom ledningsorganet, exempelvis en styrelseledamot, vid användning av tredje part för kritiska aktiviteter och/eller i betydande omfattning. Finansiella aktörer ska även ha tillräcklig personal och teknisk kapacitet inom dess verksamhet.

Finansiella aktörer ska integrera ett ramverk för tredjepartsrisker i det övergripande riskhanteringssystemet. Ramverket ska innehålla rutiner för tillsyn, riskbedömning, kontrakt, övervakning, beslut och rapportering. Vid omfattande användning av tredjepartsleverantörers tjänster bör en strategi dokumenteras, regelbundet granskas och vara i linje med affärsstrategin. Innan avtal ingås med tredjepartsleverantörer ska finansiella aktörer dokumentera en risk-, kostnads- och nyttoanalys.

2.3. Principer om relationen med tredjepartsleverantörer

Företag ska genomföra en noggrann granskning av tredjepartsleverantörer före ingående, ändring eller förnyelse av avtal. Detta gäller även för underleverantörer och ska dokumenteras och uppdateras vid behov.

Företag ska även ha personal med kompetens att övervaka tredjepartsleverantörer, där resursfördelning ska stå i proportion till tjänstens kritikalitet. Tillsynsmyndigheter bör kontrollera att rapporter om tredjepartsövervakning granskas av ledningen och att fysiska inspektioner genomförs vid behov.

2.4. Principer om särskilda risker och frågor

Tredjepartsleverantörers geografiska placering är av betydelse. Om leverantörer befinner sig i tredje länder kan detta medföra särskilda risker, exempelvis rättsliga risker, tillsynsaspekter eller operativa begränsningar. Riskerna ska beaktas i riskbedömningen, avtalen och övervakningen.

Ledningen ansvarar för att interna kontrollfunktioner avseende tredjepartsleverantörer är oberoende. Sådan användning ska vara motiverad och stå i proportion till verksamhetens

omfattning och risknivå. Det ska även finnas exitstrategier, kontroller och rutiner för att säkerställa att kontrollfunktioner fungerar effektivt vid tredjepartsanvändning.

Finansiella aktörer ska även säkerställa att tredjepartsarrangemang inte hindrar tillsyn, åtkomst eller revision av verksamhet, data, system, lokaler, personal och underleverantörer.

3. Sammanfattning

ESMA:s principer belyser finansiella aktörers ansvar vid användning av tredjepartsleverantörer. Finansiella aktörer ska upprätthålla effektiv styrning och riskhantering. Tillsynsmyndigheter ska övervaka tredjepartsrisker, säkerställa att tillsynens kvalitet inte påverkas och hantera koncentrations- och geografiska risker. Styrelse och ledning får inte delegera ansvar för styrning eller andra nyckelfunktioner inom verksamheten och ska även besitta relevant kompetens för att övervaka tredjepartsrelationer. Avtal med tredjepartsleverantörer ska föregås av en noggrann riskbedömning och uppföljning, med rutiner för kontroll, rapportering och exitstrategier.

4. HSA Söderqvist Advokatbyrås rekommendationer

HSA Söderqvist Advokatbyrå rekommenderar finansiella aktörer att integrera tredjepartsrisker i verksamhetens riskhantering. Det är av betydelse att utföra noggranna granskningar av leverantörer innan avtal ingås, ändras eller förnyas. Eventuella underleverantörer bör även granskas och löpande kontrolleras, där uppföljningen styrs av var företaget har bedömt att riskerna är som störst. Resurser för kontroll och uppföljning bör stå i proportion till tredjepartstjänstens betydelse för verksamheten. Vid användning av kritiska eller omfattande tredjepartstjänster bör en ansvarig person utses inom ledningsorganet.

Finansiella aktörer bör även beakta geografiska risker genom att identifiera och hantera rättsliga, operativa och tillsynsmässiga risker vid användning av leverantörer utanför EU.

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

Nyhetsbrev

Ang. Guide avseende tillsyn av tredjepartsleverantörer enligt DORA

25 september 2025

1. Bakgrund

I juni 2025 har Europeiska värdepappers- och marknadsmyndigheten publicerat principer för tillsyn av tredjepartsrisker, inklusive risker relaterade till informations- och kommunikationsteknologi (IKT), som regleras särskilt i DORA-förordningen.[1] Kort därefter, den 15 juli 2025, har de tre europeiska tillsynsmyndigheterna Europeiska värdepappers- och marknadsmyndigheten (ESMA), Europeiska bankmyndigheten (EBA) och Europeiska försäkrings- och tjänstepensionsmyndigheten (EIOPA) (Esorna) publicerat en guide avseende tillsyn av kritiska tredjepartsleverantörer enligt DORA.

Guidens syfte är att ur ett praktiskt perspektiv förklara hur Esornas tillsyn av kritiska tredjepartsleverantörer organiseras och genomförs. Den riktar sig till kritiska tredjepartsleverantörer, finansiella aktörer samt behöriga myndigheter. I detta nyhetsbrev sammanfattas centrala moment i tillsynsprocessen enligt DORA, baserat på guiden:

- Klassificering av kritiska tredjepartsleverantörer,
- riskbedömning och planering,
- granskning, samt
- rekommendationer och uppföljning.

Guiden är icke-bindande men fungerar som ett praktiskt stöd för att förstå DORA:s tillsynsramverk.

2. Klassificering av kritiska tredjepartsleverantörer

Esorna ska årligen offentliggöra en förteckning över kritiska tredjepartsleverantörer. Klassificeringen grundas på uppgifter som återfinns i registren över finansiella aktörers avtalsförhållanden med

[1] *Se nyhetsbrevet ang. ESMA:s principer för myndigheters tillsyn av tredjepartsrisker skickat den 4 juli 2025*

,

tredjepartsleverantörer av IKT-tjänster samt på annan tillgänglig information. Artikel 31 i DORA och kommissionens delegerade förordning[2] anger kriterierna för klassificeringen, som är följande:

- Systempåverkan på stabiliteten, kontinuiteten eller kvaliteten på tillhandahållandet av finansiella tjänster om tredjepartsleverantören skulle drabbas av ett omfattande driftsavbrott i tillhandahållandet av tjänster,
- påverkan på, eller betydelsen för, de finansiella aktörer som är beroende av tredjepartsleverantören av IKT-tjänster,
- finansiella aktörers beroende av tredjepartsleverantören av IKT-tjänster för kritiska eller viktiga funktioner, direkt eller indirekt via underleverantörer, samt
- graden av utbytbarhet av tredjepartsleverantörens IKT-tjänster.

Inom ramen för Esornas bedömning av vilka tredjepartsleverantörer som ska klassificeras som kritiska, utifrån de fyra kriterierna i artikel 31 i DORA, tillämpas elva delkriterier i en tvåstegsprocess. Först granskas informationsregistren från finansiella aktörer via behöriga myndigheter mot sex kvantitativa kriterier och därefter utvärderas leverantörerna mot fem kvalitativa kriterier för att avgöra om de ska klassificeras som kritiska enligt DORA.[3] Tredjepartsleverantörer som initialt klassificeras som kritiska får sex veckor på sig att lämna återkoppling och annan relevant information till Esorna. När klassificeringen är fastställd åläggs kritiska tredjepartsleverantörer att betala tillsynsavgifter till de behöriga myndigheterna. Tredjepartsleverantörer som inte klassificerats som kritiska kan ansöka om omprövning av sin klassificering.

3. Riskbedömning och planering

Varje år ska den aktuella tillsynsmyndigheten kartlägga riskprofilen för varje kritisk tredjepartsleverantör och bedöma de risker som leverantören står inför samt vilka åtgärder som har vidtagits för att hantera dessa risker. Bedömningen tar hänsyn till både interna och externa risker kopplade till de IKT-tjänster som leverantören tillhandahåller finansiella aktörer. Resultatet används för att prioritera tillsynsinsatser och ligger till grund för både leverantörers individuella tillsynsplan och den årliga strategiska planen som omfattar samtliga kritiska tredjepartsleverantörer.

4. Granskning

Tillsynen utförs av den gemensamma undersökningsgruppen (Joint Examination Team) bestående av medarbetare från Esorna, behöriga myndigheter för finansiella aktörer och de myndigheter som

[2] Digital Operational Resilience Regulation - European Commission
[3] *Delkriterierna framgår av figur 5 i guiden, se"Figure 5: Criticality assessment criteria"*

,

enligt NIS-regleringen[4] utövar tillsyn över kritiska tredjepartsleverantörer. Tillsynen omfattar både **kontinuerlig översyn** av kritiska tredjepartsleverantörer och **granskningar enligt den årliga tillsynsplanen**, genom **generella utredningar** eller **platsinspektioner**. Vid oförutsedda händelser, såsom incidenter eller nya hot, kan myndigheterna begära ytterligare information för att avgöra om en inspektion eller annan utredande åtgärd är nödvändig. Guiden beskriver dessa tillsynsaktiviteter i detalj, se avsnitt 5.3.1–5.3.5.

Om den aktuella tillsynsmyndigheten inte kan uppnå tillsynsmålen genom kontakt med en tredjepartsleverantörs dotterbolag i EU eller enbart genom tillsynsverksamhet i lokaler inom unionen, får myndigheten utöva sina befogenheter i lokaler belägna i ett tredjeland. Lokalerna måste ägas eller användas av en kritisk tredjepartsleverantör som tillhandahåller tjänster till finansiella aktörer inom EU. Ytterligare krav framgår i guiden.

5. Rekommendationer och uppföljning

Efter granskningar ska den aktuella tillsynsmyndigheten utfärda rekommendationer till kritiska tredjepartsleverantörer och följa upp att rekommendationerna efterlevs. Varje rekommendation kopplas till en specifik observation från granskningen, vilket tydliggör vilka områden som behöver åtgärdas för att uppfylla DORA-kraven. Tillsynsramverket föreskriver en särskild roll för behöriga myndigheter i uppföljningen. Eftersom de utövar tillsyn över finansiella aktörer säkerställer de att identifierade risker följs upp korrekt för aktörer som använder tjänster från kritiska tredjepartsleverantörer. Som en del av uppföljningen kan de aktuella tillsynsmyndigheterna även begära att behöriga myndigheter rapporterar sin bedömning av vilken effekt som rekommendationerna har på de finansiella aktörerna.

Om en kritisk tredjepartsleverantör inte följer rekommendationerna kan leverantörens identitet offentliggöras, tillsammans med information om typ och omfattning av bristen på efterlevnaden av DORA. Den aktuella tillsynsmyndigheten kan dessutom ge vägledande yttranden till behöriga myndigheter och som sista åtgärd kan den behöriga myndigheten kräva att en finansiell aktör upphör med att använda leverantörens tjänst.

6. HSA Söderqvist Advokatbyrås rekommendationer

HSA Söderqvist Advokatbyrå rekommenderar att finansiella aktörer fortsätter att integrera tredjepartsrisker i sin löpande riskhantering. Tillsynsramverket för kritiska tredjepartsleverantörer

[4] *Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS) och Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).*

,

ställer höga krav på leverantörerna, vilket i sin tur medför ansvar för finansiella aktörer som har avtal med sådana leverantörer. Det är därför av stor vikt att noggrant granska leverantörer innan avtal ingås, ändras eller förnyas. För avtal som redan finns med kritiska tredjepartsleverantörer bör löpande övervakning ske, med särskild uppmärksamhet på om behöriga myndigheter uppmärksammar leverantörers bristande efterlevnad av DORA. Vid sådana situationer bör den finansiella aktören utvärdera relationen med leverantören och vid behov vidta åtgärder, såsom att tillfälligt eller permanent avsluta avtalet. Mot bakgrund av detta kan det även vara relevant att planera för alternativa lösningar och underleverantörer för att minska sårbarheten.

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