Tjänsteutlåtande
Utfärdat 2026-05-19
Ärendenummer FGL-2026-00005

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

Regelefterlevnadsfunktionens rapport kvartal 1 2026

Förslag till beslut

I styrelsen för Försäkrings AB Göta Lejon:

Styrelsen antecknar regelefterlevnadsfunktionens rapport kvartal 1 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 1 2026

Beskrivning av ärendet

Information till styrelsen om regelefterlevnadsfunktionens rapport från kvartal 1 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. Första kvartalet har regelefterlevnadsfunktionen kontrollerat bolagets outsourcing, anpassning till nya eller förändrade regelverk samt övrig regelefterlevnad.

Regelefterlevnadsfuktionen har efter kontroll lämnat en mindre anmärkning eller synpunkt avseende att visst arbete kvarstår med att ta fram vissa tilläggsavtal med IKT-leverantörer samt att vissa leverantörer uppvisat svårighet med att efterleva redan uppdaterade IKT-avtal.

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 januari 2026 - 31 mars 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 första 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.

- IMY:s beslut mot Sportadmin i Skandivanien AB
- FI ger SBB sanktion för brister i koncernredovisningen
- Krishantering och ändrade rörelseregler för försäkringsföretag
- Cybersäkerhetslagen

2.2. Kontroll av Bolagets regelefterlevnad

Metod

Periodens kontroll har till övervägande del bestått i att följa upp Bolagets anpassning till DORA-förordningen, vilket innefattar bl.a. kontroll av revideringar i processer och riktlinjer, samt uppföljning av avtalsanpassningar.

Vidare har kontrollen innefattat uppföljning och kontroll avseende outsourcing och då primärt fokuserat på kontroll av riktlinjer samt Bolagets rutiner för uppföljning och kontroll av leverantörer. Därtill har Funktionen kontrollerat Bolagets riktlinjer för avbrottsfri verksamhet för att säkerställa att Bolaget kan upprätthålla en avbrottsfri verksamhet.

Funktionen för regelefterlevnad har vidare följt upp den tidigare anmärkningen beträffande Bolagets anpassningar till DORA-förordningen avseende primärt justerade riktlinjer och avtal med leverantörer.

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
- DORA-förordningen
- Riktlinjer för uppdragsavtal inklusive underlag för kontraktsuppföljning
- Riktlinjer för avbrottsfri verksamhet
- IKT-riktlinjer

Outsourcing - kontroll

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

Därtill har funktionen följt upp Bolagets uppföljningsprocess avseende IKT-leverantörer. Processen bedöms vara fullgod och även innebära att Bolaget har möjlighet att begära relevant dokumentation för uppföljning från såväl leverantörer som underleverantörer inom ramen för de tjänster som Bolaget köper in.

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 har för avsikt att följa upp detta under det andra kvartalet.

Anpassning till nya eller förändrade regelverk - kontroll

Uppföljning och kontroll av Bolagets anpassning till dels DORA-förordningen, dels omarbetningen av Solvens II-direktivet. Kontrollen har syftat till att säkerställa att Bolaget har anpassat rutiner och processer efter de nya regelverken.

Beträffande anpassningen till DORA-förordningen så är detta arbete färdigställt sett till justeringar i policydokument och hantering av leverantörer samt register. Likaså att börja arbeta utefter de dokumenterade processerna för avtalsuppföljning och leverantörskontroll, samt säkerställa att nästintill alla IKT-avtal är på plats med de justeringar som behövs.

Funktionen för regelefterlevnad har inte haft några synpunkter med anledning av kontrollen, med undantag för vad som i avsnittet ovan nämns om vissa IKT-avtal.

Övrig regelefterlevnad - kontroll

Uppföljning och kontroll av Bolagets riktlinjer för avbrottsfri verksamhet. Kontrollen har syftat till att säkerställa att riktlinjerna följer relevanta regler.

Funktionen har tagit del av och granskat Bolagets riktlinjer för avbrottsfri verksamhet inklusive bilagor. Funktionen för regelefterlevnad har inte haft några synpunkter på utformningen av riktlinjerna, samt kan konstatera att dessa reviderats för att efterleva DORA-förordningen.

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. Deltagande vid styrelsemöte

Funktionen för regelefterlevnad har den 22 januari 2026 deltagit vid styrelsemöte i Bolaget och därvid redogjort för föregående års årsrapport samt innevarande års årsplan.

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 20 april 2026

Johan Grenefalk

1 Översikt regelefterlevnad för kvartal 1, 2026

	Område	*Kontroll*	*Anmärkning*
	Outsourcing	Uppdragsavtal	*Ingen anmärkning.*
		Uppdragstagare	*Ingen anmärkning.*
	Anpassning till nya eller förändrade regelverk	Europaparlamentets och Rådets förordning om digital operativ motståndskraft för finanssektorn (DORA)	Visst arbete kvarstår alltjämt med Bolagets IKT-avtal, se notering i kvartalsrapporten, avsnitt 2.2.
	Övrig regelefterlevnad	Avbrottsfri verksamhet	*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 2025.*

*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

Ang. IMY:s beslut mot Sportadmin i Skandinavien AB

---

26 januari 2026

1. Inledning

Integritetsskyddsmyndigheten (IMY) har den 26 januari 2026 efter tillsyn enligt Dataskyddsförordningen[1] meddelat beslut mot Sportadmin i Skandinavien AB, nedan Sportadmin. Beslutet avser en personuppgiftsincident som inträffat i januari 2025 och som omfattat personuppgifter för drygt två miljoner personer, huvudsakligen barn och ungdomar. IMY har konstaterat att Sportadmin har brustit i sina skyldigheter enligt artikel 32.1 Dataskyddsförordningen genom att inte ha vidtagit lämpliga tekniska och organisatoriska säkerhetsåtgärder och har därför beslutat att påföra bolaget en administrativ sanktionsavgift om sex miljoner kronor.

Beslutet är av särskilt intresse ur ett dataskyddsrättsligt perspektiv eftersom det ger vägledning om hur kravet på en riskbaserad säkerhetsnivå enligt Dataskyddsförordningen ska tillämpas i praktiken.

2. Bakgrund till incidenten och IMY:s tillsyn

Sportadmin tillhandahåller digitala kommunikationstjänster till idrottsföreningar, bland annat för medlemshantering, fakturering och intern kommunikation. I januari 2025 utsattes bolagets system för ett dataintrång genom en extern angripare. Intrånget genomfördes den 16 januari 2025 genom en så kallad SQL-injektion via en variabel i en av Sportadmins webbsidor som saknade skydd mot denna typ av attacker. Av utredningen framgår att upprepade försök till SQL-injektioner hade förekommit redan dagarna innan intrånget upptäcktes.

Sårbarheten har uppkommit i samband med en kodändring i juni 2022, då en befintlig variabel återanvänts utan att omfattas av bolagets skydd mot SQL-injektioner. Den oskyddade variabeln har därefter använts direkt vid kommunikation med databasen, vilket möjliggjort intrånget. På grund av alltför generösa behörigheter i de berörda systemen kunde angriparen

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

,

bereda sig tillgång till servermiljön och föra ut data. Den 14 mars 2025 har den uthämtade informationen, innehållande personuppgifter, publicerats på Darknet.

IMY:s tillsyn har fokuserat på huruvida Sportadmin, före och vid tidpunkten för incidenten, hade vidtagit sådana säkerhetsåtgärder som krävs enligt artikel 32 Dataskyddsförordningen för att skydda de personuppgifter som behandlats i bolagets tjänster.

3. Kravet på lämpliga skyddsåtgärder och IMY:s riskbedömning

Enligt artikel 32.1 Dataskyddsförordningen ska personuppgiftsansvariga och personuppgiftsbiträden vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är anpassad till riskerna med behandlingen. Bedömningen ska göras utifrån bland annat behandlingens art, omfattning och ändamål samt de risker som behandlingen innebär för de registrerades rättigheter och friheter. IMY framhåller i beslutet att Dataskyddsförordningen bygger på ett riskbaserat angreppssätt och att kravet inte är ett absolut skydd mot alla incidenter, utan att vidtagna åtgärder ska vara proportionerliga och tillräckliga i ljuset av kända eller förutsebara risker.

IMY har bedömt att behandlingen i Sportadmins tjänster varit förenad med särskilt höga risker, främst mot bakgrund av det stora antalet registrerade, att merparten av dessa varit barn samt att behandlingen omfattat både känsliga personuppgifter och särskilt skyddsvärda uppgifter såsom personnummer. Ett obehörigt röjande eller obehörig åtkomst till dessa uppgifter skulle enligt IMY medföra allvarliga konsekvenser för de registrerade, vilket ställt krav på en hög säkerhetsnivå och effektiva skyddsåtgärder.

Mot denna bakgrund har IMY identifierat tre omständigheter som sammantaget visar att Sportadmin inte har vidtagit tillräckliga tekniska och organisatoriska säkerhetsåtgärder. För det första har bolagets förebyggande skydd ansetts vara otillräckligt. Trots att risker för SQL-injektioner varit kända under flera år har en oskyddad variabel kvarstått i systemen till följd av en kodändring redan år 2022. Sportadmin hade dessutom avstått från att införa ytterligare skyddslager, såsom web application firewall (WAF), och tillämpat alltför generösa behörigheter, vilket bidragit till att intrångets omfattning blivit större än nödvändigt.

För det andra har IMY konstaterat brister i bolagets förmåga att upptäcka svagheter i redan vidtagna säkerhetsåtgärder. Den aktuella sårbarheten har varken identifierats vid kodgranskning eller vid senare säkerhetsgenomlysningar, trots att den enligt IMY varit av grundläggande karaktär och borde ha upptäckts genom löpande uppföljning.

,

IMY konstaterar att Sportadmins säkerhetsåtgärder för övervakning inte varit tillräckliga för att upptäcka eller varna för intrångsförsöken i ett tidigt skede. Intrångsförsöken har inletts den 14 januari 2025 men uppmärksammats först den 16 januari 2025, när servrarna slutat svara. Mot bakgrund av de höga riskerna i verksamheten bedömer IMY att Sportadmin borde ha haft ett övervakningssystem som möjliggjort automatisk identifiering av intrång eller intrångsförsök i nära realtid, i syfte att tidigare kunna begränsa konsekvenserna för de registrerade.

4. Vad innebär beslutet för företagen?

IMY:s beslut mot Sportadmin tydliggör att kraven enligt artikel 32 Dataskyddsförordningen är höga, särskilt i verksamheter som behandlar stora mängder personuppgifter om barn och andra särskilt skyddsvärda uppgifter. Beslutet klargör att identifierade risker inte får stanna vid övergripande bedömningar, utan måste leda till faktiska, verifierbara och kontinuerligt uppföljda säkerhetsåtgärder.

Beslutet visar att kända risker inte kan tillåtas bestå över tid. I Sportadmins fall hade risker för SQL-injektioner identifierats under flera år utan att bolaget säkerställt att samtliga delar av systemen faktiskt omfattats av relevanta skyddsåtgärder. För företag innebär detta att riskanalyser i sig inte är tillräckliga, utan måste kompletteras med systematiska kontroller som säkerställer att åtgärder är korrekt implementerade och fungerar i praktiken, även vid kodändringar och i tekniskt komplexa miljöer.

Beslutet understryker även vikten av strukturerade rutiner för kodgranskning, förändringshantering och behörighetsstyrning. Subjektiva eller informella granskningsprocesser är inte tillräckliga när risknivån är hög. Företag förväntas i stället ha tydliga krav på granskning, använda automatiserade säkerhetstester och regelbundet se över behörigheter i syfte att begränsa konsekvenserna av ett eventuellt intrång. Vidare klargörs att restriktiv behörighetsstyrning är en grundläggande säkerhetsåtgärd, eftersom alltför generösa rättigheter kan få stor betydelse för ett intrångs omfattning.

Slutligen visar beslutet att förmåga till övervakning i nära realtid är en förväntad del av ett lämpligt säkerhetsskydd vid höga risker. Att enbart förlita sig på manuell logggranskning i efterhand är otillräckligt. Förmågan att snabbt upptäcka och reagera på intrång eller intrångsförsök kan vara avgörande för att begränsa såväl skador för de registrerade som företagets ansvar enligt Dataskyddsförordningen.

,

5. HSA Söderqvist Advokatbyrås rekommendationer

HSA Söderqvist Advokatbyrå rekommenderar att företag bör se över sina rutiner kring de tekniska och organisatoriska åtgärder som vidtas enligt artikel 32 Dataskyddsförordningen, för att bedöma om dessa är ändamålsenliga i förhållande till de risker som personuppgiftsbehandlingen innebär. Särskild uppmärksamhet bör ägnas åt hur identifierade risker hanteras i praktiken i hela systemmiljön, hur kodändringar granskas och följs upp, hur behörigheter begränsas samt om det finns förutsättningar att i ett tidigt skede upptäcka och hantera intrång eller intrångsförsök. En sådan översyn kan bidra till att stärka skyddet för personuppgifter och minska konsekvenserna av eventuella incidenter.

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

Nyhetsbrev

Ang. FI ger SBB sanktion för brister i koncernredovisningen

19 februari 2026

1. Inledning

Den 18 februari 2026 meddelade FI beslut om att ge Samhällsbyggnadsbolaget i Norden AB (SBB) en erinran samt att påföra bolaget en sanktionsavgift om 80 miljoner kronor med anledning av brister i bolagets koncernredovisning för räkenskapsåret 2021. Beslutet avser överträdelser av bestämmelserna om regelbunden finansiell information enligt lagen (2007:528) om värdepappersmarknaden.

FI:s granskning visar att SBB har redovisat fastigheter till för höga värden samt felaktigt klassificerat vissa förvärv som tillgångsförvärv i stället för rörelseförvärv. Dessa brister har medfört att koncernens resultat före skatt redovisades cirka 3,6 miljarder kronor för högt.

FI bedömer att felen varit väsentliga och att de rimligen kan ha påverkat investerares och andra intressenters beslut.

2. Bakgrund till ärendet och FI:s redovisningstillsyn

SBB är ett svenskt aktiebolag vars aktier är upptagna till handel på Nasdaq Stockholm och står därmed under FI:s tillsyn avseende regelbunden finansiell information samt de internationella redovisningsstandarder[1] som antagits av Europeiska kommissionen. Bolaget är moderbolag i en koncern vars affärsidé är att äga, förvalta, renovera och bygga samhällsfastigheter i Norden.

Ett svenskt aktiebolag, vars aktier är upptagna till handel på en reglerad marknad, ska följa de bestämmelser om regelbunden finansiell information som finns i 16 kap. lagen (2007:528) om värdepappersmarknaden. FI har tillsyn över att dessa bestämmelser följs, men har överlämnat den löpande övervakningen av den finansiella rapporteringen till Nämnden för svensk redovisningstillsyn, som är ett sakorgan under Föreningen för god sed på värdepappersmarknaden.

[1] *De internationella redovisningsstandarder som avses, enligt artikel 2 i IAS-förordningen, är International Accounting Standards (IAS-standarder) och International Financial Reporting Standards (IFRS-standarder) med tillhörande tolkningar från Standard Interpretations Committee (SIC) och International Financial Reporting Interpretations Committee (IFRIC).*

,

I det aktuella ärendet konstaterade nämnden efter sin granskning att SBB:s koncernredovisning för 2021 inte hade upprättats i enlighet med gällande regler och att bristerna inte var av ringa betydelse. Ärendet överlämnades därför till FI som därefter under 2023 inledde en egen undersökning och genomförde en självständig prövning av om bolaget hade åsidosatt sina skyldigheter som följer av 16 kap. lagen (2007:528) om värdepappersmarknaden.

3. Värdering av fastigheter till verkligt värde

3.1. FI:s iakttagelser

Under 2020 och 2021 förvärvade SBB två större fastighetsportföljer i Norge, de så kallade LV- och TB-fastigheterna[2], som huvudsakligen bestod av förskolefastigheter med långsiktiga hyresavtal.

LV-fastigheterna förvärvades 2020 för 4 750 miljoner kronor och värderades till 7 250 miljoner kronor vid utgången av 2021. TB-fastigheterna förvärvades i december 2021 för 4 977 miljoner kronor och värderades tre veckor senare till 6 670 miljoner kronor. Vid värderingarna tillämpade SBB låga direktavkastningskrav, vilket ledde till uppskrivningar under 2021.

Fastigheterna bedömdes som jämförbara när det gäller kassaflöden, hyresavtal och riskprofil, men värderades med olika avkastningskrav. Enligt SBB berodde skillnaderna på variationer i hyresavtalens längd.

Värderingarna baserades på nivå 3-indata, det vill säga icke observerbara marknadsuppgifter, som huvudsakligen hämtades från jämförelsetransaktioner av andra typer av fastigheter. Uppgifter från bolagets eget förvärv av TB-fastigheterna gavs begränsad betydelse.

3.2. FI:s bedömning

I FI:s bedömning använde SBB inte den under omständigheterna bästa tillgängliga informationen vid värderingen av TB- och LV-fastigheterna. Bolaget borde ha utgått från det egna förvärvet av TB-fastigheterna, som var en ordnad transaktion och motsvarade verkligt värde vid förvärvstidpunkten. De 21 dagar som förflöt mellan förvärv och värdering motiverade inte att förvärvspriset gavs begränsad betydelse.

[2] *Fastigheterna förvärvades från företaget TB (TB-fastigheterna) respektive företaget LV (LV-fastigheterna).*

,

FI ansåg vidare att uppgifterna från TB-förvärvet även borde ha använts vid värderingen av LV-fastigheterna, eftersom fastigheterna var mycket jämförbara. Genom att inte göra detta redovisades fastigheterna till för höga värden.

Enligt FI innebar detta att koncernens resultat före skatt för 2021 redovisades cirka 3,6 miljarder kronor för högt, vilket motsvarar omkring 12 procent. Felen bedömdes som väsentliga och innebar att koncernredovisningen inte hade upprättats i enlighet med de internationella redovisningsstandarderna IAS 40, IAS 8 och IAS 1 samt artikel 4 i IAS-förordningen.

4. Redovisning av förvärv som tillgångsförvärv

4.1. FI:s iakttagelser

Under 2021 fick SBB bestämmande inflytande över Offentliga Hus i Norden AB och Amasten Fastighets AB, två börsnoterade fastighetsbolag med anställda, löpande verksamhet och omfattande fastighetsbestånd i Sverige.

Vid förvärven genomförde SBB ett koncentrationstest enligt IFRS 3 och bedömde att de förvärvade fastigheterna utgjorde likartade tillgångar. Förvärven redovisades därför som tillgångsförvärv.

Av uppgifter som SBB lämnat till FI framgår att om förvärven i stället hade redovisats som rörelseförvärv skulle goodwill ha uppgått till cirka 1,2 miljarder kronor för Amasten och cirka 1,1 miljarder kronor för Offentliga Hus, samt uppskjuten skatt till cirka 2,4 miljarder kronor respektive 1,5 miljarder kronor.

Bedömningen grundades på vissa kvalitativa och kvantitativa riskegenskaper, såsom fastighetstyp, storlek, geografisk spridning, hyresgäster och direktavkastningskrav, vilka varierade mellan 3,6 och 7,6 procent för Offentliga Hus och mellan 1,85 och 5,85 procent för Amasten.

4.2. FI:s bedömning

FI bedömde att kriterierna i koncentrationstestet inte var uppfyllda vid förvärven av Offentliga Hus och Amasten, eftersom fastigheterna hade olika typer, lägen, hyresgäster och riskprofiler. De kunde därför inte anses utgöra likartade tillgångar.

FI konstaterade vidare att båda bolagen vid förvärvstidpunkten utgjorde rörelser. De omfattade fastigheter, anställda, hyresavtal och löpande förvaltningsprocesser som var

,

nödvändiga för att generera hyresintäkter. Den löpande fastighetsförvaltningen bedömdes som en betydande process, och de förvärvade verksamheterna innehöll organiserade arbetsstyrkor med nödvändig kompetens.

Enligt FI borde förvärven därför ha redovisats som rörelseförvärv enligt IFRS 3. Genom att i stället redovisa dem som tillgångsförvärv uteblev redovisning av goodwill, uppskjuten skatt och föreskrivna upplysningar.

FI bedömde att dessa fel var väsentliga. Goodwill och uppskjuten skatt som inte redovisats uppgick till betydande belopp, och nödvändiga upplysningar saknades trots att de förvärvade fastigheterna utgjorde en väsentlig del av koncernens tillgångar. Bristerna bedömdes rimligen ha påverkat de beslut som användarna av koncernredovisningen fattar på grundval av rapporten samt haft betydande påverkan på den övergripande bilden av bolagets finansiella ställning.

Sammanfattningsvis fann FI att koncernredovisningen för 2021 inte hade upprättats i enlighet med tillämpliga bestämmelser och att SBB därmed hade åsidosatt sina skyldigheter.

HSA Söderqvist Advokatbyrås rekommendationer

HSA Söderqvist Advokatbyrå rekommenderar att företag bör beakta följande mot bakgrund av FI:s beslut. Bestämmelserna om regelbunden finansiell information är centrala för att säkerställa ett gott investerarskydd. Brister i redovisningen kan försämra investerares möjligheter att fatta välgrundade beslut och riskerar att undergräva förtroendet för värdepappersmarknaden.

Mot denna bakgrund bör företag:

- säkerställa att finansiell rapportering och värderingar sker i enlighet med gällande regelverk och tillsynspraxis,
- dokumentera väsentliga antaganden, modeller och bedömningar på ett transparent sätt, samt
- upprätthålla en effektiv intern kontroll och löpande uppföljning av den finansiella informationen.

Genom detta kan företag minska risken för tillsynsåtgärder, stärka investerarskyddet och bidra till en välfungerande kapitalmarknad.

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

Nyhetsbrev

Ang. Krishantering och ändrade rörelseregler för försäkringsföretag

---

24 februari 2026

1. Krishantering och ändrade rörelseregler för försäkringsföretag

Regeringen har i betänkandet *SOU 2025:97 Krishantering och ändrade rörelseregler för försäkringsföretag* presenterat förslag till hur det nya EU-direktivet om återhämtning och resolution för försäkringsföretag[1] (IRRD) samt ändringar i Solvens II-direktivet[2] ska genomföras i svensk rätt. Finansinspektionen har i sitt remissvar den 12 januari 2026 i huvudsak tillstyrkt förslagen, men samtidigt framhållit behovet av vissa förtydliganden och justeringar. Den 16 februari 2026 har även den europeiska försäkrings- och tjänstepensionsmyndigheten EIOPA publicerat utkast till riktlinjer och tekniska standarder för genomförandet av IRRD.

Förslagen innebär sammantaget en omfattande reform av direktivet för försäkringsföretag, med ökat fokus på krisberedskap, riskhantering och långsiktig finansiell stabilitet. Samtidigt föreslås vissa undantag från kraven för mindre och icke-komplexa företag.

IRRD och ändringarna av Solvens II-direktivet ska börja tillämpas den 30 januari 2027.

2. Föreslagna ändringar i Solvens II-direktivet

2.1. Hållbarhetsrisker i riskhanteringen

De föreslagna ändringarna i Solvens II-direktivet innebär att hållbarhetsrisker tydligare integreras i försäkringsföretagens riskhantering. Företagen ska ha strategier, riktlinjer, processer och system för att identifiera, mäta, hantera och följa upp miljörelaterade, sociala

---

[1] *Europaparlamentets och rådets direktiv (EU) 2025/1 av den 27 november 2024 om inrättande av en ram för återhämtning och resolution av försäkrings- och återförsäkringsföretag och om ändring av direktiven 2002/47/EG, 2004/25/EG, 2007/36/EG, 2014/59/EU och (EU) 2017/1132 och förordningarna (EU) nr 1094/2010, (EU) nr 648/2012, (EU) nr 806/2014 och (EU) 2017/1129.*

[2] *Europaparlamentets och rådets direktiv (EU) 2025/2 av den 27 november 2024 om ändring av direktiv 2009/138/EG vad gäller proportionalitet, tillsynskvalitet, rapportering, långsiktiga garantiåtgärder, makrotillsynsverktyg, hållbarhetsrisker samt grupptillsyn och gränsöverskridande tillsyn, och om ändring av direktiven 2002/87/EG och 2013/34/EU.*

och styrningsrelaterade risker på kort, medellång och lång sikt. Definitioner av hållbarhetsrisker och hållbarhetsfaktorer kommer att införas i försäkringsrörelselagen.

Vidare ska försäkringsföretag upprätta särskilda planer med kvantifierbara mål och tydliga processer för att övervaka och beakta de finansiella risker som uppstår till följd av hållbarhetsfaktorer. Planerna ska ta hänsyn till EU:s klimat- och omställningsmål och följas upp löpande, med närmare krav som preciseras genom tekniska standarder. Företagen ska dessutom årligen offentliggöra de mål som ingår i planerna.

Kraven på planer för hantering av hållbarhetsrisker ska anpassas efter företagets affärsmodell samt arten, omfattningen och komplexiteten i dess hållbarhetsrisker. Målen, förfarandena och åtgärderna i planerna ska därför stå i proportion till den riskexponering som företaget har.

2.2. Styrdokument om ersättning och mångfald

Direktivet ställer krav på att försäkringsföretag ska ha styrdokument om ersättning och mångfald. Företagen ska anta ett styrdokument som främjar mångfald i styrelsen, bland annat genom mål om en jämn könsfördelning, samt tydliga riktlinjer för ersättningssystemen. Syftet är att stärka bolagsstyrningen och motverka osunda incitament.

2.3. Plan för likviditetshantering

Enligt de nya förslagen ska försäkringsföretag upprätta och regelbundet uppdatera en plan för likviditetsriskhantering för att förebygga och hantera betalningsproblem. Planen ska visa hur företaget klarar sina in- och utbetalningar på kort sikt i förhållande till tillgångar och skulder, hur det agerar vid ekonomisk stress samt innehålla en kortsiktig analys av inkommande och utgående kassaflöden.

Planen ska lämnas in till Finansinspektionen och kan på myndighetens begäran behöva utvidgas till att även omfatta medellång och lång sikt. Ett försäkringsföretag som använder en matchningsjustering eller volatilitetsjustering ska få kombinera en plan för likviditets-riskhantering med en likviditetsplan.

Små och icke-komplexa företag kan undantas från detta krav, och företag som ingår i en koncern kan i vissa fall omfattas av en gemensam plan på gruppnivå.

2.4. Oberoende mellan centrala funktioner

Reglerna om centrala funktioner förtydligas. Som huvudregel ska olika personer ansvara för riskhantering, regelefterlevnad, aktuariefunktion och internrevision för att minska risken för

,

intressekonflikter. Mindre och icke-komplexa företag kan i vissa fall kombinera funktioner, dock inte internrevisionen, och endast om intressekonflikter kan hanteras på ett tillfredsställande sätt.

2.5. SFCR-rapport och ORSA

Ändringarna i Solvens II-direktivet innebär även förändringar i rapporteringen. Solvens- och verksamhetsrapporten (SFCR) delas upp i två delar. Den ena delen riktar sig till försäkringstagare och ska innehålla lättillgänglig information om företagets verksamhet, riskprofil, solvenssituation och hållbarhetsrisker. Den andra delen riktar sig till branschaktörer och tillsynsmyndigheter och innehåller mer detaljerad information om bolagsstyrning, riskhantering och värderingsmetoder.

Vidare införs krav på att Solvens II-balansräkningen ska granskas av en oberoende revisor. Revisorn ska säkerställa att uppgifterna är korrekta och upprättade enligt gällande standarder samt lämna en särskild granskningsrapport till Finansinspektionen. Detta stärker kvaliteten och tillförlitligheten i den finansiella rapporteringen.

Inom ramen för ORSA skärps kraven på analys av makroekonomiska faktorer. Försäkringsföretagen ska, utifrån sin risknivå och verksamhetens komplexitet, analysera den makroekonomiska utvecklingen och situationen på finansmarknaderna, inklusive hur konjunkturnedgångar, börsfall och andra negativa händelser kan påverka solvensen. Större och mer riskutsatta företag förväntas genomföra mer avancerade analyser, medan små och icke-komplexa företag kan omfattas av förenklade krav eller undantag.

ORSA ska dessutom omfatta en bedömning av företagets samlade betalningsförmåga. Det innebär att företaget inte bara ska ha tillräckligt kapital, utan även tillräcklig likviditet för att fullgöra sina betalningsförpliktelser under både normala och stressade marknadsförhållanden.

2.6. Sanktionssystemet

Det nuvarande taket på 50 miljoner kronor för sanktionsavgifter avskaffas. I stället ska avgiftens storlek bestämmas på samma sätt som enligt andra regelverk på finansmarknadsområdet, exempelvis 15 kap. 8 § lagen om bank- och finansieringsrörelse. Detta innebär att sanktionsavgiften kan anpassas efter överträdelsens allvar, omfattning och företagets storlek.

,

2.7. Förlagslån

Utredningen föreslår att försäkringsföretag ska få använda förlagslån, dvs. efterställda skulder, i större utsträckning för att stärka sin kapitalbas, upp till åtta procent av primärkapitalet. Syftet är att ge företagen ökad flexibilitet i sin kapitalstruktur.

Finansinspektionen avstyrker dock förslaget i dess nuvarande utformning. Avstyrkandet avser förslagets konkreta utformning och motivering och innebär inte ett generellt ställningstagande mot framtida lättnader i lånebegränsningsreglerna. Finansinspektionen anser att frågan bör analyseras närmare innan eventuella förändringar genomförs.

2.8. Långsiktiga aktieinvesteringar och kapitalkrav

Förslaget innebär att försäkringsföretag, efter godkännande från Finansinspektionen, får tillämpa ett lägre kapitalkrav för vissa aktieinnehav som hålls långsiktigt. För att omfattas av lättnaden måste företaget visa att investeringarna är stabila och inte behöver avyttras vid marknadsoro eller kriser. Om kraven inte längre uppfylls ska företaget vidta åtgärder, annars förloras rätten att använda metoden. Syftet är att främja långsiktigt sparande och bidra till ökad finansiell stabilitet.

3. Ett nytt ramverk för krishantering och resolution

Genom införandet av EU:s krishanteringsdirektiv för försäkringsföretag (IRRD) stärks direktivet för hantering av finansiella kriser inom försäkringssektorn. Direktivet syftar till att säkerställa att företag i svårigheter kan återhämta sig eller avvecklas på ett ordnat sätt, utan att försäkringstagare drabbas i onödan eller att den finansiella stabiliteten äventyras.

Enligt de nya reglerna ska försäkringsföretag upprätta detaljerade återhämtningsplaner som beskriver hur verksamheten kan stabiliseras vid olika typer av krissituationer. Planerna ska innehålla så kallade ”tänk om”-scenarier och utgöra en integrerad del av företagens styrning och riskhantering.

Samtidigt ges tillsyns- och resolutionsmyndigheterna utökade befogenheter att ingripa i ett tidigt skede om ett företag hamnar i finansiella svårigheter. Detta kan exempelvis ske genom krav på omorganisation, kapitalåtgärder eller andra stabiliserande insatser. Direktivet stärker även det gränsöverskridande samarbetet mellan myndigheter genom ökat informationsutbyte och samordning.

I Sverige genomförs direktivet genom en ny lag om resolution av försäkringsföretag (resolutionslagen). Lagen reglerar förutsättningarna för resolution, ansvarsfördelningen mellan myndigheter och de verktyg som kan användas vid en kris. I praktiken innebär

,

regleringen inte några omedelbara förändringar i den dagliga verksamheten, men den ställer ökade krav på företagens förberedelser och krisberedskap.

Sammantaget innebär IRRD ett skifte från reaktiv krishantering till ett mer förebyggande och strukturerat arbetssätt, med fokus på motståndskraft, stabilitet och skydd för försäkringstagare.

Den 16 februari 2026 har EIOPA publicerat det första paketet med riktlinjer och utkast till tekniska standarder för genomförandet av IRRD. Paketet omfattar bland annat vägledning om innehållet i förebyggande återhämtningsplaner, kriterier för vilka företag som ska upprätta sådana planer, krav på innehåll i resolutionsplaner, samt kriterier för identifiering av kritiska funktioner och bedömning av resolvabilitet. Syftet med riktlinjerna och standarderna är att stödja en enhetlig och praktisk tillämpning av direktivet i hela EU och att underlätta för både försäkringsföretag och tillsynsmyndigheter att förbereda sig inför IRRD:s ikraftträdande år 2027.

HSA Söderqvist Advokatbyrås rekommendationer

HSA Söderqvist Advokatbyrå rekommenderar att försäkringsföretag, mot bakgrund av de föreslagna regeländringarna och den fortsatta implementeringsprocessen, redan nu påbörjar sitt anpassningsarbete, även om direktivet befinner sig i ett tidigt skede. Regeringen kommer förhoppningsvis under sommaren eller i höst att lägga fram en proposition som ytterligare klargör hur kraven slutligt kommer att utformas i svensk lag. Under året väntas även kompletterande riktlinjer och tekniska standarder som preciserar tillämpningen i praktiken.

Företagen bör se över sina styrnings- och riskhanteringssystem, särskilt avseende integreringen av hållbarhetsrisker i befintliga processer och styrdokument, vilket även kan underlätta arbetet inom ORSA. Vidare bör företagen säkerställa att kraven på makroekonomiska analyser och bedömningen av den samlade betalningsförmågan inom ORSA uppfylls och är anpassade till verksamhetens riskprofil.

Vidare rekommenderas att företagen genomför en översyn av sina centrala funktioner, styrdokument för ersättningar och mångfald samt rutiner för rapportering och intern kontroll, för att säkerställa att organisationen och styrningen är anpassade till de nya kraven.

Företag som kan komma att omfattas av kraven på återhämtnings- och resolutionsplaner bör i ett tidigt skede kartlägga kritiska funktioner, interna beroenden och möjliga krisscenarier, samt säkerställa att relevanta beslutsprocesser och ansvarsfördelningar är tydligt dokumenterade.

,

HSA Söderqvist Advokatbyrå kommer att bevaka utvecklingen på EU-nivå och den fortsatta lagstiftningsprocessen noggrant, inklusive EIOPA:s riktlinjer och tekniska standarder, och löpande informera om hur dessa påverkar försäkringsföretagens verksamhet.

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

Nyhetsbrev

Ang. Cybersäkerhetslagen

2 mars 2026

1. Bakgrund

Den nya cybersäkerhetslagen (2025:1506) har trätt i kraft den 15 januari 2026 och innebär att NIS2-direktivet[1] införlivats i svensk rätt. Lagen syftar till att stärka cybersäkerheten i samhällskritisk verksamhet och omfattar ett brett spektrum av sektorer, däribland bankverksamhet och finansmarknadsinfrastruktur. Föreskrifter förväntas ges ut under våren 2026.

Jämfört med det tidigare NIS-direktivet omfattar regelverket fler sektorer och verksamheter samt innebär ett tydligare ansvar, särskilt avseende riskbedömningar, säkerhetsåtgärder, incidenthantering och ledningens ansvar. För många organisationer medför detta nya skyldigheter, bland annat krav på registrering och ett mer systematiskt informationssäkerhetsarbete.

Inledningsvis kan konstateras att cybersäkerhetslagen inom finanssektorn främst tar sikte på vissa särskilt angivna verksamhetsutövare, vilka redogörs för i avsnitt 2. Under sektorn finansmarknadsinfrastruktur anges bland annat operatörer av handelsplatser samt centrala motparter. Finansiella entiteter som inte tillhör dessa kategorier omfattas som utgångspunkt inte av direktivets tillämpningsområde inom denna sektor. Bedömningen ska dock göras med beaktande av verksamhetens faktiska funktion, organisatoriska roll och rättsliga klassificering.

För många aktörer inom finanssektorn, däribland fondbolag, värdepappersbolag och försäkringsföretag, innebär detta att cybersäkerhetslagen typiskt sett inte blir direkt tillämplig. Dessa verksamheter regleras i stället genom DORA-förordningen, som har företräde framför cybersäkerhetslagen i frågor som rör bland annat riskhantering och incidentrapportering.

[1] *Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen.*

,

2. Tillämpningsområde

Cybersäkerhetslagen gäller för verksamheter inom 18 särskilt utpekade sektorer. Dessa delas in i två kategorier:

Högkritiska sektorer: energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, digital infrastruktur, förvaltning av IKT-tjänster mellan företag, offentlig förvaltning och rymdverksamhet.

Andra kritiska sektorer: post- och budtjänster, avfallshantering, tillverkning, produktion och distribution av kemikalier, produktion, bearbetning och distribution av livsmedel, digitala leverantörer, forskning och tillverkningsindustri.

Gällande ”finansmarknadsinfrastruktur”[2] utpekas två typer av entiteter:

- Operatör av handelsplatser: en reglerad marknad, en MTF-plattform eller en OTF-plattform.
- Centrala motparter: juridiska personer som träder emellan motparterna i kontrakt som är föremål för handel på en eller flera finansmarknader och blir köpare till varje säljare och säljare till varje köpare.

En verksamhetsutövare som bedriver verksamhet inom någon av dessa sektorer och är lika stor som eller större än ett medelstort företag omfattas av cybersäkerhetslagen.

Även mindre verksamheter kan omfattas, exempelvis om de är den enda leverantören i Sverige av en tjänst som är avgörande för att upprätthålla samhällsviktig eller ekonomiskt kritisk verksamhet. Under vissa förutsättningar omfattas också statliga myndigheter, regioner och kommuner. Som huvudregel gäller lagens krav för hela verksamheten hos en verksamhetsutövare som omfattas av lagen, och alltså inte enbart för den del av verksamheten som tillhör en utpekad sektor.

3. Vad innebär cybersäkerhetslagen?

Cybersäkerhetslagen syftar till att uppnå en hög nivå av cybersäkerhet i samhället genom att införa ett harmoniserat regelverk för verksamhetsutövare som anses ha betydelse för samhällsviktig verksamhet. Lagen innehåller bestämmelser om verksamhetsutövares skyldigheter, tillsyn samt ingripanden vid bristande efterlevnad.

För de verksamhetsutövare som omfattas av lagen innebär regelverket i huvudsak följande.

[2] *Bilaga I till NIS2-direktivet.*

,

Verksamhetsutövare ska anmäla sin verksamhet till behörig tillsynsmyndighet och löpande uppdatera uppgifter när förändringar sker. Företag inom sektorerna bankverksamhet och finansmarknadsinfrastruktur som identifierar sig som leverantörer av samhällsviktiga tjänster ska anmäla detta till Myndigheten för civilt försvar (MCF) via myndighetens anmälningsportal. De uppgifter som lämnas vid anmälan kommer att tillhandahållas Finansinspektionen.

Vidare ska verksamhetsutövare vidta lämpliga och proportionella tekniska, organisatoriska och driftsrelaterade säkerhetsåtgärder för att skydda nätverks- och informationssystem mot incidenter. Åtgärderna ska baseras på en samlad och riskbaserad bedömning av verksamhetens cybersäkerhetsrisker och bland annat omfatta riskanalys, incidenthantering, kontinuitetsplanering, säkerhet i leveranskedjan samt styrning av åtkomst och informationssäkerhet.

Lagen ställer även krav på ledningsnivå. Personer i verksamhetsutövarens ledning ska genomgå utbildning i säkerhetsåtgärder och ha tillräcklig förståelse för cybersäkerhetsrisker och hur dessa ska hanteras inom verksamheten.

Vid betydande incidenter ska verksamhetsutövaren utan dröjsmål underrätta tillsynsmyndigheten, i regel inom 24 timmar från det att incidenten upptäckts, följt av en mer fullständig incidentanmälan inom föreskriven tidsfrist samt efterföljande rapportering.

Efterlevnaden av lagen står under tillsyn, och vid överträdelser kan tillsynsmyndigheten besluta om förelägganden, andra ingripanden samt administrativa sanktionsavgifter. Sanktionsavgifterna kan uppgå till betydande belopp och bestäms bland annat utifrån verksamhetsutövarens storlek och klassificering.

4. DORA har företräde framför cybersäkerhetslagen

DORA-förordningen har företräde framför cybersäkerhetslagen i vissa delar, bland annat avseende incidentrapportering. Finansiella entiteter som omfattas av cybersäkerhetslagen ska därför fortsatt rapportera allvarliga IKT-relaterade incidenter till Finansinspektionen i enlighet med DORA.

Finansinspektionen vidarebefordrar därefter rapporterade incidenter till Myndigheten för civilt försvar för de verksamhetsutövare som har anmält att de omfattas av cybersäkerhetslagen. Syftet är att möjliggöra informationsdelning mellan berörda myndigheter utan att införa dubbla rapporteringsskyldigheter för finansiella entiteter.

,

5. HSA Söderqvist Advokatbyrås rekommendationer

Även om cybersäkerhetslagen som utgångspunkt inte är direkt tillämplig på fondbolag, värdepappersbolag och andra finansiella entiteter som omfattas av DORA-förordningen, är regelverket relevant eftersom det bygger på samma riskbaserade principer, ingår i samma tillsynsstruktur och kan påverka myndigheternas praktiska tolkning av cybersäkerhetskrav. Vi har därför mycket att lära av cybersäkerhetslagen och den tillsyn som sker av de sektorer som ingår i arbetet med DORA. Det är således relevant att följa utvecklingen på området, inklusive kommande praxis och myndighetsvägledning.

HSA Söderqvist Advokatbyrå kommer att bevaka detta och dela med oss av lärdomar för att underlätta tolkning och tillämpning av DORA.