Till
Styrelsen i S:t Erik Livförsäkring AB

Rapport för perioden 1 januari - 16 februari 2022 avseende regelefterlevnad

1 Inledning

Genom denna rapport redovisar funktionen för regelefterlevnad resultatet av senast genomförd kontroll av S:t Erik Livförsäkring 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.

- DORA-förordningen.
- IMY:s sanktionsavgifter mot Region Uppsala.
- Nytt direktiv för återhämtning och resolution av försäkringsföretag.

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)*
Rapportering	Rapportering till Finansinspektionen.	Kontrollen har inte föranlett några synpunkter.
Övrig regelefterlevnad	IT-säkerhet, cyberrisker och informationssäkerhet.	Kontrollen har inte föranlett några synpunkter.
	Avbrottsfri verksamhet.	Kontrollen har inte föranlett några synpunkter.
	Efterlevnad av riktlinjer för riskhantering	Kontrollen har inte föranlett några synpunkter.

Rapportering

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

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

Kontrollen har inte föranlett några synpunkter.

Övrig regelefterlevnad

a) Uppföljning av Bolagets implementering av EIOPA:s regler om informationssäkerhet och IKT-risker. Kontrollen har syftat till att säkerställa ändamålsenliga rutiner och riktlinjer i enlighet med för Bolaget gällande regler avseende dessa områden.

   Bolaget har redogjort för arbetet och dess tillvägagångsätt avseende bl.a. processer och rapporteringsvägar för att säkerställa god informationssäkerhet och IT-säkerhet. Funktionen för regelefterlevnad har vidare granskat relevanta styrdokument avseende informationssäkerhet och avbrottsfri verksamhet utan synpunkter.

Då EIOPA:s regelverk alltjämt är nytt och Bolaget löpande kommer att behöva se över rutiner och processer avser funktionen för regelefterlevnad att fortsatt följa upp frågan med Bolaget under året.

Kontrollen har inte föranlett några synpunkter.

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

   Funktionen för regelefterlevnad har överenskommit med Bolaget att invänta granskning av dokumentet tills detta har antagits ånyo av styrelsen under våren 2022.

2.3 Deltagande vid styrelsemöte

Funktionen för regelefterlevnad har inte deltagit vid något styrelsemöte under den aktuella perioden.

2.4 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

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 16 februari 2022

Johan Grenefalk

Bilaga 1

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. DORA-förordningen

---

26 januari 2022

Förordning om digital operativ motståndskraft i den finansiella sektorn, nedan DORA, som EU-kommissionen tog fram till förslag i september 2020 har nu antagits. DORA innehåller krav som innebär att merparten av de aktörer som är aktiva i den finansiella sektorn ska bli mer motståndskraftiga mot informations- och kommunikationsrelaterade (IKT) störningar och hot. Några utestående punkter kommer att förhandlas innan det slutliga förslaget antas, vilket kan ta upp till nio månader. Därefter kommer det även att tas fram tekniska standarder till DORA. Nedan sammanfattas några av de krav som följer av DORA.

- *Tillämpningsområde*: DORA omfattar de flesta finansiella aktörerna under Finansinspektionens tillsyn med ett fåtal undantag. De enda aktörerna som undantas är systemoperatörer och systemdeltagare såvida de inte själva är en finansiell enhet som regleras på unionsnivå och som sådan ska omfattas av DORA.

- *Styrning och riskhantering*: Det ställs krav på att organisation och ledning har kontroll över hur IKT-risker hanteras, både i förhållande till interna system och utkontrakterade system. Aktörer som omfattas av DORA måste genom policyer, strategier och processer säkerställa att all relevant infrastruktur, inklusive servrar, lokaler, datacenter och hårdvara, är tillräckligt skyddade för att förhindra fysisk skada, obehörig åtkomst eller utnyttjande. Ramverket ska ses över varje år och uppdateras efter behov.

- *IKT-klassificering*: IKT-funktioner ska klassificeras och risker kopplade till IKT-funktioner ska identifieras. Tredjepartsrisker ska ingå som en integrerad del av de finansiella aktörernas IKT-riskramverk. IKT-incidenter ska klassificeras utifrån vissa faktorer såsom hur många motparter som drabbades av incidenten, långvarighet, graden av allvarlighet och om kritiska system var föremål för incidenten samt incidentens ekonomiska effekter.

- *Testning av IKT-säkerhet*: I DORA finns även krav på testprogram och avancerade penetrationstester som ska simulera en cyberattack och på så vis identifiera brister i IKT-system. Tekniska standarder ska tas fram avseende dels vilka typer av finansiella aktörer som ska omfattas av dessa tester, dels om testerna som sådana.

- *Hantering av IKT-tredjepartsrisker*: DORA innehåller bestämmelser som syftar till att möjliggöra övervakning av kritiska tredjepartsleverantörer av IKT-tjänster. Syftet är att

etablera ett gemensamt forum för övervakning under de europeiska tillsynsmyndigheternas gemensamma kommitté. Vidare ställs det krav på de avtal som reglerar förhållandet till tredjepartsleverantörer.

- *Rapportering av IKT-incidenter*: DORA innehåller en skyldighet att rapportera cyberhot som skulle kunna resultera i en betydande IKT-incident. Betydande IKT-incidenter ska rapporteras till behöriga myndigheter inom vissa bestämda tidsramar. Tekniska standarder kommer att tas fram med mer detaljerade bestämmelser om klassificering och gränsvärden för vilka incidenter som ska betraktas som betydande incidenter. Det kan noteras att förslaget om harmoniserad rapportering innebär att finansiella aktörer, som i dag är skyldiga att rapportera IKT-incidenter till Myndigheten för samhällsskydd och beredskap (MSB) i enlighet med NIS-direktivet, endast behöver rapportera incidenter definierade enligt den föreslagna nya DORA-förordningen och tillhörande tekniska standarder till Finansinspektionen.

- *Proportionalitet*: EU-kommissionen har framhållit att proportionalitetsprincipen präglar DORA-förordningen och innebär att samma krav inte ställs på s.k. mikroföretag när det gäller styrning och hantering av IKT-risker. Mikroföretag är företag som sysselsätter färre än tio personer och där omsättningen eller balansomslutningen inte överstiger två miljoner euro per år. Dessutom är kraven på riskhantering riskbaserade, vilket innebär att högre komplexitet medför högre krav på riskhantering, och vice versa.

- Finansinspektionen ska inte vara samrådsmyndighet enligt förslagen i det slutbetänkande som Cybersäkerhetsutredningen överlämnat avseende DORA. I stället ska säkerhetspolisen eller Försvarsmakten vara samrådsmyndighet. Eftersom Finansinspektionen är tillsynsmyndighet enligt säkerhetsskyddslagen innebär det i praktiken att två olika myndigheter ges befogenhet att ingripa mot en och samma verksamhetsutövare för överträdelser av dess skyldigheter enligt säkerhetsskyddslagen. Detta har Finansinspektionen reagerat på och uttryckt att för det fall att tillsyn och samråd ska ske med olika myndigheter bör det framgå av säkerhetsskyddsförordningen, eller annan lämplig författning, hur samverkan ska ske mellan myndigheter.

Sammanfattningsvis syftar DORA till att stärka den finansiella sektorns motståndskraft mot IKT-risker, inte att höja förlusttäckningsgraden i händelse av en IKT-händelse. De bestämmelser som ingår i DORA är således av kvalitativ natur och berör inte kapitalkrav.

Wesslau Söderqvist Advokatbyrås rekommendationer

Regelkraven kring informations- och cybersäkerhet ökar för finansiella aktörer liksom även riskerna för att utsättas för exempelvis ransomeware. Wesslau Söderqvist Advokatbyrå uppmuntrar därför finansiella aktörer att redan nu säkerställa att tillräckliga skyddsåtgärder vidtas i syfte att efterleva DORA och minska risken för IKT-incidenter. Inledande skyddsåtgärder kan exempelvis var att se över interna rutiner, riktlinjer och processer för att identifiera vilka IKT-risker och IKT-tillgångar som finns i verksamheten. Därefter behöver arbete läggas ned för att säkerställa att riskerna kan hanteras på ett ändamålsenligt sätt. I detta arbete vill Wesslau Söderqvist Advokatbyrå understryka att även budget för informationssäkerhet samt vilka typer av försäkringar som finns och vad dessa täcker i händelse av informations- och cyberrelaterade incidenter bör beaktas i riskhanteringsarbetet.

Wesslau Söderqvist Advokatbyrå kommer att fortsätta bevaka lagstiftningsarbetet kring DORA och andra regerverk avseende informations- och cybersäkerhet.

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

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. Integritetsskyddsmyndighetens sanktionsavgifter mot Region Uppsala

---

1 februari 2022

1 Inledning

1.1 Bakgrund

Integritetsskyddsmyndigheten, nedan IMY, mottog i maj 2019 två rapporter om att Region Uppsala hade skickat känsliga personuppgifter utan kryptering till mottagare både i och utanför Sverige. Med anledning av detta inledde IMY en granskning av regionstyrelsen och sjukhusstyrelsen i Uppsala.

Till följd av granskningarna har IMY genom två separata beslut utfärdat sanktionsavgifter om sammanlagt 1 900 000 kronor mot Region Uppsala. Till grund för besluten låg Region Uppsalas bristande säkerhetsåtgärder vid hantering av känsliga personuppgifter.

1.2 GDPR - Art. 32.1

I båda besluten var det Art. 32.1 GDPR som låg i huvudfokus. Artikeln stadgar i korthet att personuppgiftsansvariga och personuppgiftsbiträden ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken för personer och deras rättigheter. I detta ingår bl.a. att, när det är lämpligt, pseudonymisera och kryptera personuppgifter. Vid bedömningen av en lämplig säkerhetsnivå är utgångspunkten de risker som behandlingen medför, t.ex. förstöring-, ändring-, förlust-, obehörig åtkomst- och röjande av personuppgifter.

2 IMY:s beslut

2.1 Beslut mot regionstyrelsen

Granskningen av regionstyrelsen avsåg perioden den 25 maj 2018 till den 7 maj 2019. Granskningen avsåg både automatiska och manuellt skickade e-postmeddelanden som innehöll patientuppgifter. E-postmeddelandena hade skickats internt inom organisationen och inte nått några externa mottagare. E-postmeddelandena hade skickats för administration, kvalitetssäkring, forskning och kvalitetsuppföljning.

Regionstyrelsen hade vid tiden för överträdelserna interna styrdokument som stadgade att känsliga personuppgifter inte fick kommuniceras via e-post. Överföringarna av e-postmeddelandena var i sig krypterade – däremot var innehållet, som fanns i excelfiler, inte krypterat.

IMY förklarade att personuppgifter om hälsa är känsliga personuppgifter som kan innebära betydande risker för den personliga integriteteten. Behandlingarna innehöll även personnummer som anses vara särskilt skyddsvärda personuppgifter, sådana uppgifter kräver ett starkt skydd. På grund av detta var det inte tillräckligt att endast kryptera överföringen av meddelandena. En adekvat skyddsnivå hade t.ex. varit att även kryptera informationen i e-postmeddelandena.

IMY konstaterade därmed att det saknades tekniska skyddsåtgärder för att förhindra läsning, ändring samt obehörig åtkomst av informationen. Inte heller hade tillräckliga organisatoriska åtgärder företagits eftersom riskerna hade identifierats genom interna styrdokument, men trots det inte efterföljts. Region Uppsala hade därav inte säkerställt en lämplig säkerhetsnivå i enlighet med Art. 32.1 i GDPR.

Vid en samlad bedömning ansåg IMY att 300 000 kronor var en lämplig sanktionsavgift mot bakgrund av överträdelserna. Försvårande omständigheter var bl.a. att det avsåg en stor mängd okrypterad information med känsliga personuppgifter och personnummer, att e-postmeddelandena hade skickats systematiskt över en längre tid samt att behandlingarna skett i strid med interna riktlinjer. Förmildrande omständigheter som beaktades var bl.a. att överföringen i sig varit krypterad och att e-postmeddelandena endast skickats internt inom regionen.

2.2 Beslut mot sjukhusstyrelsen

Granskningen av sjukhusstyrelsen avsåg samma period, från den 25 maj 2018 till den 7 maj 2019. Granskningen avsåg skickade e-postmeddelanden med patientuppgifter till patienter och remittenter, dvs. hemsjukhuset, i tredjeland. Granskningen omfattade även lagring av patientuppgifter i e-postvårdtjänsten i Outlook. Även sjukhusstyrelsen hade interna styrdokumenten om att känsliga personuppgifter inte fick kommuniceras via e-post.

Personuppgifterna skickades okrypterade över öppet nät, dvs. via internet. Varken överföringen av e-postmeddelandena eller informationen var i detta fall skyddad av kryptering. Visserligen användes OTLS (ett kryptografiskt kommunikationsprotokoll) vid överföringen men OTLS fungerar endast om mottagaren har samma version av protokollet och detta kunde inte

sjukhusstyrelsen säkerställa hos mottagaren. I september 2019, dvs. efter granskningsperioden, införde emellertid sjukhusstyrelsen en krypteringslösning som möjliggjorde en säker överföring.

Likt ovanstående beslut var det ett stort antal personuppgifter som exponerats för betydliga risker. Detta hade skett under en längre tid och utan adekvata tekniska- och organisatoriska skyddsåtgärder. I detta fall var överträdelserna av allvarligare slag då personuppgifterna även exponerats mot internet. Bristen i säkerheten var därav av sådant allvarligt slag att både Art. 5.1 f och Art. 32.1 i GDPR hade överträtts.

Vid en samlad bedömning ansåg IMY att 1 600 000 kronor var en lämplig sanktionsavgift mot bakgrund av överträdelserna. Försvårande omständigheter var bl.a. att det hade rört sig om en stor mängd okrypterad information innehållande känsliga personuppgifter och personnummer, att informationen hade skickats systematiskt över en längre tid, att behandlingarna skickats via öppet nät och lagrats i Outlook samt att behandlingarna skett i strid med interna riktlinjer. Förmildrande omständigheter som beaktades var att sjukhusstyrelsen efter granskningsperioden infört tekniska åtgärder i form av en krypteringslösning för filer.

3 Wesslau Söderqvist Advokatbyrås rekommendationer

Wesslau Söderqvist Advokatbyrå rekommenderar till följd av ovanstående att bolag som hanterar personuppgifter säkerställer att bolagets interna GDPR-riktlinjer efterföljs.

I dagsläget har de flesta bolag tagit fram interna GDPR-riktlinjer – vilket förstås är positivt. Sanktionsbesluten från IMY visar dock på att det är minst lika viktigt med både rutiner och kontroller som säkerställer att de interna riktlinjerna dels motsvarar den faktiska personuppgiftshanteringen, dels efterföljs på ett korrekt sätt. Wesslau Söderqvist Advokatbyrå rekommenderar därför att interna processer granskas och jämförs med skriftliga interna riktlinjer. Det är också viktigt att belysa de interna riktlinjerna inom organisationen för att minimera riskerna att de inte efterföljs. Detta kan bl.a. uppfyllas genom olika utbildningsinsatser.

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

Nyhetsbrev

Ang. Nytt direktiv för återhämtning och resolution av försäkringsföretag

---

9 februari 2022

EU-kommissionen har lämnat förslag till ett nytt direktiv för återhämtning och resolution av försäkringsföretag (IRRD). Direktivet ska förse myndigheter med system och verktyg för att i ett tidigt stadium kunna ingripa för det fall ett försäkringsföretag fallerar, eller sannolikt kommer att fallera, i syfte att skydda försäkringstagarna och det finansiella systemet. Motsvarande direktiv finns redan bl.a. för kreditinstitut och värdepappersföretag.

Den kanske största, och mest kontroversiella, förändringen i och med det nya direktivet är införandet av en resolutionsmyndighet för försäkringsföretag. Resolutionsmyndigheten ska utarbeta resolutionsplaner där de anger vilka åtgärder de avser att vidta om villkoren för resolution – vilka anges i direktivet (se stycket nedan) – är uppfyllda. Om förslaget godkänns förväntas närmare 20 svenska försäkringsföretag tilldelas resolutionsplaner av myndigheten.

Enligt förslaget ska ett försäkrings- eller återförsäkringsföretag försättas i resolution när det fallerar eller sannolikt kommer att fallera och det inte finns några utsikter till att alternativ från privata sektorn eller tillsynsåtgärder kan förhindra fallissemang. I dessa fall får resolutionsmyndigheten befogenhet att tillämpa resolutionsverktyg på företaget, däribland försäljning av verksamhet, avskiljande av tillgångar och skulder, solvent avveckling samt nedskrivning eller konvertering av kapitalinstrument och kvalificerade skulder.

Utöver det ovanstående behöver försäkringsföretag även utarbeta återhämtningsplaner innehållande åtgärder för att återställa den finansiella ställningen om den försämrats avsevärt, detta är således ett verktyg för att undvika att företaget når resolutionsvillkoren ovan. Enligt förslaget ska minst 80 procent av en medlemsstats marknad omfattas av sådana krav, uppskattningsvis ca 30 svenska försäkringsföretag enligt Svensk Försäkring. Både resolutions- och återhämtningsplanerna skulle innebära betydande arbetsinsatser för försäkringsföretagen.

I nuläget behöver inga åtgärder vidtas med anledning av förslaget, däremot är det värdefullt att vara förberedd på det ovannämnda. Förslaget förhandlas inom EU-rådet och EU-parlamentet och vid ett eventuellt godtagande har det föreslagits att det ska träda i kraft 18 månader efter godkännandet.

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

Wesslau Söderqvist Advokatbyrå i Stockholm KB
Kungsgatan 36, Box 7836, 103 98 Stockholm, Sweden, Tel +46(0)8-407 88 00
Org.nr 969692-4969, info@wsa.se, www.wsa.se