Göteborgs Stad

Beslutsunderlag
Utfärdat 2022-04-12
Diarienummer 0000/22

Handläggare
Katrin Gundersen
Telefon: 031-368 55 12
E-post: katrin.gundersen@gotalejon.goteborg.se

Regelefterlevnadsrapport, kvartal 1, 2022

Förslag till beslut i styrelsen för Försäkrings AB Göta Lejon

- anteckna regelefterlevnadsrapporten kvartal 1, 2022.

Sammanfattning

Regelefterlevnadsfunktionen lämnar varje år fyra rapporter varav en är en sammansatt kvartalsrapport från kvartal 4 och en slutlig årsrapport. Granskningen genomförs och har sin grund i den plan som regelefterlevnadsfunktionen upprättar årligen och som godkänns av styrelsen för ett år i taget.

Rapporten från första kvartalet har 6 avvikelser varav 1 är grön och resterande gula.

Bedömning ur ekonomisk dimension

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

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.

Samverkan

Ingen samverkan har genomförts

Bilagor

1. Regelefterlevnadsrapport kvartal 1, 2022.

Ärendet

Anteckna rapport från regelefterlevnadsfunktionen kvartal 1, 2022

Beskrivning av ärendet

Granskningen genomförs och har sin grund i den plan som regelefterlevnadsfunktionen upprättar årligen och som godkänns av styrelsen för ett år i taget.

Förvaltningens /bolagets bedömning

Det är bolagets bedömning att de rekommendationer som har noterats av regelefterlevnadsfunktionen är rimliga och att bolaget kommer att åtgärda dessa.

Till
Styrelsen i Försäkrings AB Göta Lejon

Kvartalsrapport för perioden 1 januari - 31 mars 2022 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 första kvartalet 2022.

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

- DORA-förordningen.
- IMY:s sanktionsavgifter mot Region Uppsala.
- Nytt direktiv för återhämtning och resolution av försäkringsföretag.
- Finansinspektionens sanktionsbeslut mot Trustly Group AB och ClearOn AB.

2.2 Kontroll av Bolagets regelefterlevnad

IT- och informationssäkerhet

Uppföljning och kontroll av Bolagets IT- och informationssäkerhet inklusive rutiner för avbrottsfri verksamhet. Kontrollen har syftat till att dels följa upp tidigare rekommendationer med anledning av nya regelverk under år 2021, dels säkerställa att Bolaget har fullgoda rutiner avseende ovan.

Bolaget har vid möte redogjort för arbetet för att upprätthålla en god nivå på arbetet kring informationssäkerhet innefattande avbrottsfri verksamhet och IT-säkerhet. Bolaget har upprättat riktlinjer för IKT (Informations- och kommunikationsteknik) baserade på EIOPA:s riktlinjer för att stärka detta arbete.

Under år 2021 har Bolaget mottagit en rapport från Transcendent Group AB som omfattar Bolagets arbete med IKT och informationssäkerhet. I rapporten återspeglas ett antal brister, vilka Bolaget arbetar med att åtgärda. Funktionen för regelefterlevnad har vidare föreslagit justeringar i riktlinjerna för IKT, för att dessa ska vara så anpassade till verksamheten som möjligt. I anslutning till granskningen av riktlinjerna har funktionen för regelefterlevnad även rekommenderat att Bolagets styrelse på ett tydligare sätt ska dokumentera riskanalys och strategi avseende IKT och informationssäkerhet.

Bolaget har meddelat att arbetet fortlöper väl med att implementera dels EIOPA:s regler, dels med att komma till rätta med tidigare förslag och rekommendationer. Funktionen för regelefterlevnad har i anslutning till kontrollen påbörjat en granskning av rutiner och planer för krisberedskap m.m., detta för att säkerställa en avbrottsfri verksamhet. Dessa ska antas av styrelsen i april 2022 och kommer slutligt att granskas därefter.

Funktionen för regelefterlevnad kommer att följa upp detta område under nästa kvartal.

Försäkringsverksamhet

Uppföljning och kontroll av Bolagets produktgodkännandeprocess och produktstyrning. Kontrollen har syftat till att säkerställa att Bolaget har rutiner och riktlinjer på plats för att reglera processen vid framtagande av nya försäkringsprodukter.

Bolaget har vid kontrollmötet redogjort för den nya produkt som är under framtagande, försäkring mot olycksfall. Funktionen för regelefterlevnad har varit involverad i processen samt biträtt med översyn av anmälan till Finansinspektionen och justeringar i bolagsordningen. Bolaget har en bra rutin för att dokumentera förändringar i produktutbudet, men arbetar för närvarande med att ta fram en mer formaliserad produktgodkännandeprocess.

Funktionen för regelefterlevnad rekommenderar Bolaget att ta fram styrdokument över produktgodkännandeprocessen.

Övrig regelefterlevnad

Uppföljning och kontroll av Bolagets dokumenterade rutiner för att hantera dels klagomålshantering, dels etiska frågor.

Funktionen för regelefterlevnad har inför styrelsemötet i april 2022 granskat Bolagets samtliga styrdokument. I anslutning till granskningen har funktionen föreslagit vissa justeringar avseende riktlinjen för etiska frågor samt rekommenderat att Bolaget ska utbilda sin personal i etiska frågor. Detta kommer att följas upp under nästkommande kvartal.

Riktlinjerna för klagomålshantering har granskats utan synpunkter från funktionen för regelefterlevnad.

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 25 januari 2022 deltagit vid styrelsemöte i Bolaget och därvid redogjort för årsrapporten samt årsplanen för år 2022.

3 Funktionen för regelefterlevnads bedömning

De rekommendationer som funktionen för regelefterlevnad lämnat framgår ovan i 2.2. Utöver detta har funktionen för regelefterlevnad vid fullgörandet av sitt uppdrag inte funnit något som innebär att Bolaget sammanta get inte lever upp till de krav som uppställs i de lagar, förordningar, föreskrifter och allmänna råd som gäller för Bolagets tillståndspliktiga verksamhet.

Stockholm den 11 april 2022

Johan Grenefalk

1 Översikt regelefterlevnad för kvartal 1, 2022

	Område	*Kontroll*	*Anmärkning*
	IT- och informationssäkerhet	IT-säkerhet och informationssäkerhet inkl. cyberrisker.	Se kommentar i 2.2 i kvartalsrapporten.
		Avbrottsfri verksamhet.	Se kommentar i 2.2 i kvartalsrapporten.
	Försäkringsverksamhet	Produktgodkännandeprocess, produktstyrning.	Se kommentar i 2.2 i kvartalsrapporten.
	Övrig regelefterlevnad	Klagomålshantering.	Ingen anmärkning.
		Hantering av etiska frågor.	Se kommentar i 2.2 i kvartalsrapporten.

*Denna matris syftar till att ge Bolaget en överblick över resultatet av utförd kontroll av Bolagets regelefterlevnad samt återge vilka åtgärder 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*
	Q3 2021	IKT-anpassning	IKT-riktlinje.	De interna riktlinjerna bedöms hålla en god miniminivå, dock behöver den interna riktlinjen ses över mot bakgrund av den GAP-analys som genomförts av Transcendent Group AB där en rad brister identifierats.
	Q3 2021	ESG/hållbarhet (avvaktas)	Arbete avseende ESG och hållbarhetsfrågor.	Bolaget har ett pågående hållbarhetsarbete och tillsammans med riskfunktionen ska Bolaget fastställa strategi för hållbarhetsmål. Funktionen för regelefterlevnad avser att följa upp detta under år 2022.
	Q2 2021	Outsourcing	Beredskapsplan.	Rekommendation att Bolaget ser över Bolagets kontinuitetsplan för att säkerställa att där anges uppdaterade och relevanta uppgifter och kontaktuppgifter. Utöver ovan har KPMG i sin internrevisionsrapport 2021:1 rekommenderat att Bolaget förtydligar vem som har ansvar för att granska, uppdatera och testa kontinuitetsplanen.

				Då nya planer ska antas vid bolagets styrelsemöte i april 2022 avvaktar funktionen för regelefterlevnad att följa upp planerna till de antagits.

*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.

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

Nyhetsbrev

Ang. Finansinspektionens sanktionsbeslut mot Trustly Group AB och ClearOn AB

---

24 februari 2022

1 Inledning

Finansinspektionen, nedan FI, har meddelat två sanktionsbeslut på grund av allvarliga brister i Trustly Group AB:s och ClearOn AB:s efterlevnad av penningtvättsregelverket. Besluten har resulterat i varningar som förenats med sanktionsavgifter om 130 miljoner kronor för Trustly Group AB och 14 miljoner kronor för ClearOn AB.

Utredningarna har utförts i syfte att undersöka om Trustly Group AB och ClearOn AB följt penningtvättslagen och FI:s penningtvättsföreskrifter.[1] Gemensamt för båda besluten är att det har förelegat allvarliga brister i bolagens åtgärder för kundkännedom vid affärsförbindelser samt att överträdelserna har varit särskilt allvarliga då verksamheterna innefattat högriskområden i förhållande till penningtvätt och finansiering av terrorism.

2 Trustly Group AB

FI anser att ett allvarligt fel som påträffats i undersökningen är att Trustly Group AB inte har identifierat majoriteten av användarna som kunder till bolaget i penningtvättslagens mening. FI har konstaterat att när användare av tjänsten väljer att genomföra en betalning så är det Trustly Group AB som uppdras att genomföra betalningen och användaren behöver godkänna bolagets allmänna villkor. Av villkoren framgår det att det är Trustly Group AB, och inte slutanvändarens bank, som tillhandahåller tjänsten. Därav uppstår en affärsförbindelse enligt 1 kap. 8 § 4 penningtvättslagen och användarna är att betrakta som kunder till Trustly Group AB. Bestämmelserna avseende den allmänna riskbedömningen, riskklassificeringen, rutiner och riktlinjer samt kundkännedom har således inte efterlevts på grund av den bristande identifieringen.

Värt att notera är att i sanktionsbedömningen anser FI att handlandet omfattas av förmildrande omständigheter. Trustly Group AB har vid ett tidigare tillfälle, under år 2015, varit föremål för en utredning av FI där bolagets inställning i kundidentifieringsfrågan uppdagats – i det fallet avskrevs utredningen utan motivering. FI har därav gjort bedömningen att Trustly Group AB får

[1] *Lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen) och Finansinspektionens föreskrifter (FFFS 2017:11) om åtgärder mot penningtvätt och finansiering av terrorism.*

anses ha uppfattat att FI inte hade något att invända mot bolagets inställning till att användarna inte skulle klassificeras som kunder. Trots att överträdelserna normalt sett skulle anses vara särskilt grava så kunde de därför – i detta enskilda fall – inte betraktas som allvarliga.

Trustly Group AB har även visat på andra allvarliga brister i sin verksamhet utöver de ovanstående, bl.a. har bolaget inte inkluderat en av sina största tjänster, s.k. ”Pay N Play”, i sin allmänna riskbedömning. På flera håll har Trustly Group AB haft allvarliga brister i sina åtgärder för kundkännedom. De allvarligaste bristerna har upptäckts i samband med granskning av Trustly Group AB:s autogirokunder där bolaget helt saknat rutiner och riktlinjer för kundkännedom samt varit bristande i sin riskklassificering. Utöver det ovanstående har Trustly Group AB inte beaktat autogirokundernas geografiska etablering, vilket kan vara en ytterligare riskfaktor.

Det framgår tydligt av beslutet att FI har lagt vikt vid att betalningar inom spelbranschen, som av flera myndigheter har klassificerats som en högriskbransch avseende penningtvätt och finansiering av terrorism, står för mer än hälften av Trustly Group AB:s transaktionsvolym. Regelverket inom penningtvätt kräver att bolag har ett riskbaserat förhållningssätt. Därför krävs det att Trustly Group AB vidtar särskilt ingående åtgärder för att hantera risken som följer av bolagets affärsmodell och inriktning mot spelbranschen.

3 ClearOn AB

ClearOn AB har, som Trustly Group AB, brustit i reglerna för kundkännedom. Särskilt allvarligt är det att FI:s utredning endast omfattat de kunder som omsatt större belopp och genomfört flest kundorder och att brister förekommit i samtliga granskade kundakter.

ClearOn AB har överhuvudtaget inte riskklassificerat sina privatkunder och inom vissa områden saknar ClearOn AB dessutom helt sådana rutiner och riktlinjer som penningtvättslagen kräver. I de fall som rutiner och riktlinjer faktiskt förekommit har de på flera sätt varit bristfälliga.

Även i detta fall har FI lagt vikt vid att ClearOn AB:s verksamhet är särskilt exponerad för risker för penningtvätt och finansiering av terrorism – i detta fall eftersom verksamheten innefattar en hög grad av kontanthantering samt att bolaget erbjuder penningöverföring till utlandet.

4 Wesslau Söderqvist Advokatbyrås rekommendationer

Wesslau Söderqvist Advokatbyrå vill framhålla vikten av att penningtvättsregelverket har ett riskbaserat förhållningssätt, dvs. vilka åtgärder som behöver företas enligt regelverket beror på

vilken risknivå som aktualiseras, vilket i sin tur är beroende av verksamhetens enskilda omständigheter och egenskaper. Vidare vill Wesslau Söderqvist Advokatbyrå framhålla vikten av att kontinuerligt följa upp riskerna och löpande bedöma uppgifter om varje specifik kund under hela affärsförbindelsen.

Regelverket är på flera sätt diffust eftersom det inte finns exakta krav om t.ex. vad som krävs för att ett bolag ska anses ha uppnått tillräcklig kundkännedom vid var tid, detta är upp till aktörer som träffas av regelverket att bedöma. Det är därför värdefullt att kontinuerligt kartlägga de olika riskfaktorerna som kan innebära att kraven ställs högre. Om riskerna ökar ställs högre krav på ökad kundkännedom och uppföljning. I detta fall exemplifieras kontanthantering och typ av bransch men många andra faktorer spelar också roll såsom t.ex. storlek på transaktioner, geografisk etablering, kategori av kund, omfattning av tidigare misstänka transaktioner och beteenden.

I de nu aktuella sanktionsbesluten har Trustly Group AB och ClearOn AB visat på väldigt tydliga brister eftersom bolagen inom flera områden helt saknar åtgärder samt rutiner och policys. Det kan därmed förmodas att oavsett vilken bransch som verksamheten exponerats mot eller huruvida kontanthantering förekommit inom verksamheten så hade troligtvis FI valt att ingripa ändå – däremot kan det presumeras att sanktionsbeloppen har påverkats av verksamheternas särskilda riskfaktorer.

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