Beslutsunderlag
Utfärdat 2021-09-13
Diarienummer 0013/21

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

Rapport regelefterlevnadsfunktionen kvartal 2, 2021

Förslag till beslut

I styrelsen för Försäkrings AB Göta Lejon:

- Anteckna rapport från regelefterlevnadsfunktionen kvartal 2, 2021.

Sammanfattning

Genom denna rapport återkopplar funktionen för regelefterlevnad resultatet av senaste genomförda kontrollen av *Försäkrings AB Göta Lejon. Överblick över utfallet av revisionen finns beskrivet i bilaga 1.

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

Underlag för granskning har tagits fram i samverkan med bolagsjuristen och regelefterlevnadsfunktionen.

Bilagor

1. Rapport regelefterlevnadsfunktionen kvartal 2, 2021.
2. Bilaga 1 Översikt över rekommendationer
3. Bilaga 2 Sammanfattning nyhetsuppdateringar

Ärendet

Styrelsen ska kvartalsvis informeras om de granskningar som genomförts i bolaget i enlighet med den plan som styrelsen fastställer årligen.

Beskrivning av ärendet

Rapporten har tagits fram efter granskning av följande områden:

1. Utlagd verksamhet
2. IKT anpassning
3. ESG/hållbarhet
4. IDD
5. Klagomålshantering

Bolagets bedömning

Det är bolagets bedömning att rapporten alla delar stämmer med planen för granskning.

WESSLAU SÖDERQVIST

Till
Styrelsen i Försäkrings AB Göta Lejon

Kvartalsrapport för perioden 1 april - 30 juni 2021 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 andra kvartalet 2021.

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

2 Händelser av relevans under perioden

2.1 Regelbevakning

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

- Finansinspektionen beslutar om tillägg till solvenskapitalkravet för Försäkringsbolaget PRI Pensionsgaranti.
- EU-kommissionen har antagit nya standardavtalsklausuler.
- Rapport från Integritetsskyddsmyndigheten avseende anmälda personuppgiftsincidenter under år 2020.
- Finansinspektionen meddelar sanktionsbeslut mot Maiden Life AB.

2.2 Kontroll av Bolagets regelefterlevnad

Outsourcing

a) Kontroll av Bolagets uppdragsavtal. Kontrollen har syftat till att säkerställa att Bolaget har ändamålsenliga uppdragsavtal som uppfyller kraven på innehåll i uppdragsavtal i enlighet med

försäkringsrörelselagen (2010:2043) (FRL), artikel 274.4 Kommissionens delegerade förordning (EU) 2015/35, EIOPA:s riktlinjer om uppdragsavtal med molntjänstleverantörer (EIOPA-BoS-20-002) samt EIOPA:s riktlinjer för säkerhet och företagsstyrning avseende informations- och kommunikationsteknik (EIOPA-BoS-20/600).

Bolaget har informerat funktionen för regelefterlevnad om den utlagda verksamheten samt om de anmälningspliktiga uppdragsavtal som Bolaget har med tjänsteleverantörer. Bolaget har vidare informerat om att samtliga uppdragsavtal, liksom sådana som avser molntjänster, är anmälda till Finansinspektionen.

Funktionen för regelefterlevnad har mottagit och granskat Bolagets uppdragsavtal. Flera av avtalen har behov av uppdatering för att fullt ut uppfylla ovan angivna krav. Avtalen måste minst innehålla kraven i kommissionens delegerade förordning 2015/35 om vad som ska ingå i skriftliga avtal med tjänsteleverantörer. Dessa krav framgår även av EIOPA:s riktlinjer för företagsstyrningssystem (Eiopa-Bos-14/253 SV).

Det bör i uppdragsavtalen bl.a. förtydligas att tjänsteleverantörer ska verka för att bibehålla kontinuitet i Bolagets verksamhet vid eventuell uppsägning av avtal eller andra avbrott samt att Bolaget ska kunna avsluta arrangemang utan att detta inkräktar på kontinuiteten. I vissa avtal är det inte tydligt vilken uppsägningstid som gäller för det fall en leverantör vill häva avtalet. Sådan uppsägningstid måste vara tillräckligt lång för att Bolaget ska finna alternativa lösningar. Detta bör förtydligas. Vidare saknas det i flera avtal bestämmelser som ger Bolaget och Bolagets externa revisorer samma rätt till tillgång till leverantörernas lokaler som Finansinspektionen har. Även att leverantörer ska underrätta Bolaget om leverantörens egna såväl som underleverantörers incidenter bör förtydligas.

Bolaget har påbörjat ett arbete med att se över och revidera samtliga uppdragsavtal där Wesslau Söderqvist Advokatbyrå bistår i arbetet med att granska samtliga uppdragsavtal och ta fram tilläggsavtal där detta bedöms nödvändigt. Även Bolagets personuppgiftsbiträdesavtal ses över och revideras. Funktionen för regelefterlevnad avser att följa upp arbetet med att signera nya avtal alternativt tilläggsavtal under nästkommande kvartal.

b) Kontroll av Bolagets interna rutiner och riktlinjer för utlagd verksamhet. Kontrollen syftar till att säkerställa att Bolaget har ändamålsenlig kontroll över sin utlagda verksamhet i syfte att bibehålla en god intern styrning och kontroll och efterleva för Bolaget gällande krav avseende outsourcing.

Funktionen för regelefterlevnad har tagit emot och granskat Bolagets interna riktlinjer för utlagd verksamhet. Funktionen för regelefterlevnad rekommenderar Bolaget att i den interna riktlinjen se över avsnitt 2.0 avseende innehåll i uppdragsavtal. Krav på sådant innehåll regleras huvudsakligen i Kommissionens delegerade förordning (EU) 2015/35. Den lista som återges i

Bolagets interna riktlinjer bör, i de delar listan inte överensstämmer med förordningens krav i artikel 274.4, kompletteras i syfte att säkerställa att Bolagets uppdragsavtal ges det innehåll som krävs enligt förordningen, bl.a. bör det förtydligas att samtliga uppdragsavtal ska säkerställa Bolagets rätt att erhålla information från uppdragstagaren samt att Bolaget ska kunna avsluta uppdrag utan att detta inkräktar på kontinuiteten i verksamheten. Vidare ska inte endast Finansinspektionen ges tillträde till uppdragstagarens lokaler, utan denna rättighet ska även tillfalla Bolaget samt av Bolaget utsedda revisorer.

Utöver ovan bör avsnitt 2.0 avseende innehåll i uppdragsavtal kompletteras med information om vad avtal med molntjänstleverantörer måste innehålla enligt EIOPA:s riktlinjer om uppdragsavtal med molntjänstleverantörer, se riktlinje 10 om avtalsenliga krav. Likaså finns det krav i EIOPA:s IKT-riktlinjer på vad avtal rörande IKT-tjänster och IKT-system måste innehålla, se riktlinje 25 om utkontraktering av IKT-tjänster och IKT-system.

Funktionen för regelefterlevnad har utöver ovan mottagit och granskat den checklista som Bolaget tagit fram avseende innehåll i uppdragsavtal. Samma rekommendation gäller som ovan, då denna checklista saknar några relevanta punkter som anges i EIOPA:s riktlinjer för molntjänster liksom EIOPA:s IKT-riktlinjer.

Funktionen för regelefterlevnad avser att följa upp detta under kommande kvartal.

c) Kontroll av Bolagets rutiner för uppföljning av uppdragstagare. Kontrollen har syftat till att säkerställa att Bolaget har ändamålsenliga interna rutiner för att följa upp Bolagets uppdragstagare på regelbunden basis för att säkerställa att Bolaget har kontroll över den utlagda verksamheten.

Bolaget har redogjort för de rutiner som tillämpas för att följa upp den utlagda verksamheten. Bolaget ska ha regelbundna avstämningsmöten med samtliga uppdragstagare för att följa upp den utlagda verksamheten. Bolaget har informerat funktionen för regelefterlevnad om avstämningsmöten inte har hållits med samtliga uppdragstagare år 2021. Funktionen för regelefterlevnad rekommenderar att sådana avstämningsmöten hålls regelbundet, minst årligen samt vid behov. Funktionen för regelefterlevnad rekommenderar också att sådana avstämningar dokumenteras.

Bolaget har vidare upplyst funktionen för regelefterlevnad om att det inte görs någon övergripande analys avseende den utlagda verksamheten och om behovet för att lägga ut verksamhet förändrats från tid till annan. Med anledning av att Bolaget har flera uppdragsavtal beträffande kritiska eller viktiga operativa funktioner eller verksamheter rekommenderar funktionen för regelefterlevnad att en sådan övergripande analys genomförs minst årligen i syfte

att säkerställa en god intern styrning och kontroll. Sådan analys bör inkludera en utvärdering av samtliga uppdragstagare i syfte att fånga upp eventuella brister samt för att kunna bedöma om någon verksamhet ska plockas hem eller läggas ut på ny tjänsteleverantör.

Funktionen för regelefterlevnad avser att följa upp ovanstående rekommendationer under fjärde kvartalet 2021.

d) Kontroll av Bolagets beredskapsplan. Kontrollen har syftat till att säkerställa att Bolaget har en ändamålsenlig beredskapsplan enligt 10 kap. 3 § FRL.

Bolaget har redogjort för Bolagets beredskapsplan och informerat om att kontinuitets- och beredskapsplan ska stresstestas innan årsskiftet 2021. Bolaget har vidare enligt uppgift säkerställt att Bolagets uppdragstagare har egna beredskapsplaner.

Funktionen för regelefterlevnad har vidare mottagit och granskat Bolagets kontinuitetsplan. Funktionen för regelefterlevnad rekommenderar att kontinuitetsplanen ses över under året för att säkerställa att samtliga uppgifter är korrekta. Det bör bl.a. i avsnitt 6 i kontinuitetsplanen uppdateras vilka tjänsteleverantörer som numera är kontrollfunktioner samt deras kontaktuppgifter. Funktionen för regelefterlevnad har vidare noterat att KPMG i sin internrevisionsrapport 2021:1 rekommenderat att Bolaget förtydligar vem som har ansvar för att granska, uppdatera och testa kontinuitetsplanen. Funktionen för regelefterlevnad avser att följa upp detta under kommande kvartal.

IKT-anpassning

Med anledning av att Bolaget vid tidpunkten för utförandet av kontrollen inväntar en rapport avseende informationssäkerhet och IKT avser funktionen för regelefterlevnad att följa upp detta område under nästkommande kvartal. Funktionen för regelefterlevnad har informerats om att Bolagets styrelse antagit en ny riktlinje för IKT vid styrelsemötet den 8 juni 2021. Tidigare rekommendation från Bolagets föregående funktion för regelefterlevnad om att upprätta ett sådant styrdokument är således hanterad. Funktionen för regelefterlevnad avser att granska riktlinjen under nästkommande kvartal.

ESG/hållbarhet

Kontroll av Bolagets arbete avseende ESG och hållbarhetsfrågor. Kontrollen har syftat till att följa upp hur Bolaget arbetar med hållbarhet. Bolaget har informerat funktionen för regelefterlevnad om att Bolaget har ett pågående hållbarhetsarbete och att Bolaget tillsammans med riskfunktionen ska fastställa en strategi för hållbarhetsmål. Funktionen för regelefterlevnad avser att följa upp detta arbete under nästkommande kvartal.

Bolaget omfattas inte av EU:s nya omfattande reglering avseende hållbarhetsrelaterade upplysningar som ska lämnas inom den finansiella tjänstesektorn (Disclosureförordningen och Taxonomiförordningen).

2.3 Uppföljning av utestående punkter från föregående funktion för regelefterlevnad

Funktionen för regelefterlevnad har följt upp utestående punkter som är rapporterade från Transcendent Group, som tidigare innehaft uppdraget som funktion för regelefterlevnad i Bolaget.

IDD

Transcendent Group har tidigare noterat att antalet fortbildningstimmar inte fullt ut uppnåtts, vilket ansetts som en obetydlig avvikelse med anledning av Covid-19.

Bolaget har redogjort för Bolagets rutiner för att uppnå kraven på minst 15 timmars fortbildning för de anställda som direkt deltar i Bolagets försäkringsdistribution. Några som omfattas av kravet har under våren genomfört utbildning samt kunskapstest och de återstående är inbokade att genomföra detta under hösten 2021. Funktionen för regelefterlevnad kan konstatera att Bolaget har ändamålsenliga rutiner för att efterleva kraven på minst 15 timmars fortbildning samt årligt kunskapstest för de anställda som direkt deltar i Bolagets försäkringsdistribution.

Uppföljningen har inte föranlett några synpunkter utan tidigare rekommendation från Transcendent Group får anses hanterad.

Klagomålshantering

Transcendent Group har rekommenderat Bolaget att redovisa mätbara variabler (riskaptit) i klagomålsrapporteringen så att ledningen och styrelsen kan följa upp effektiviteten i hanteringen samt kan följa upp avvikelser. Speciellt bör skaderegleringstiden mätas mot ett fast tidsmål (uppdelat på försäkringsklass), dels för att det idag anses vara en väl utdragen process, dels för att lättare kunna mätas och påverkas, något som i sin tur bör minska ryktesrisken och antal inkomna klagomål. Bolaget har informerat funktionen för regelefterlevnad om att det har pågått ett arbete med att se över och granska Bolagets klagomålshantering. Vidare har Bolaget informerat om att det fortfarande förekommer långa handläggningstider.

Funktionen för regelefterlevnad håller med om att hanteringen av klagomål har behövt en översyn och har nu mottagit samt granskat reviderade riktlinjer för såväl klagomålshantering som för överprövningsärenden. Funktion för regelefterlevnad anser att det är lämpligare att klagomål används som mätinstrument för operativ risk, istället för att detta blir en egen riskkategori som ska tillsättas en riskaptit.

Funktionen för regelefterlevnad har rekommenderat ett antal mindre justeringar i dessa riktlinjer, men tycker i övrigt att de håller god nivå. Funktionen har vidare rekommenderat att Bolaget ska säkerställa hur klagomål rapporteras från leverantörer och uppdragstagare för att Bolaget ska kunna känna sig tryggt i att Bolaget har full vetskap om eventuella inkomna klagomål.

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.

2.5 Deltagande vid styrelsemöte

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

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 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 13 juli 2021

Johan Grenefalk

1 Översikt regelefterlevnad för kvartal 2, 2021

	Område	*Kontroll*	*Anmärkning*
	Outsourcing	Uppdragsavtal.	Det pågår ett arbete med att se över och revidera Bolagets uppdragsavtal för att dessa ska efterleva gällande regelkrav på innehåll i sådana avtal. Funktionen för regelefterlevnad avser att följa upp detta under nästkommande kvartal.
		Riktlinjer för uppdragsavtal.	Rekommendation att se över avsnitt 2.0 ”Uppdragsavtalets innehåll” i riktlinjerna i syfte att det ska överensstämma med art. 274.4 den delegerade förordningen 2015/35 om krav på innehåll i uppdragsavtal. Vidare bör riktlinjerna kompletteras med vad som bör ingå i uppdragsavtal enligt relevanta riktlinjer från EIOPA avseende IKT samt molntjänster. Revidering anses nödvändig för att säkerställa att samtliga regelkrav beaktas vid framtagande av uppdragsavtal. En översyn rekommenderas även avseende Bolagets checklista för utlagd verksamhet i syfte att även fånga upp kraven i EIOPA:s riktlinjer för molntjänster samt EIOPA:s IKT-riktlinjer.
		Bolagets uppföljning av uppdragstagare.	Rekommendation att hålla minst årliga avstämningar med samtliga tjänsteleverantörer samt dokumentera dessa avstämningar. Vidare rekommenderas att det minst årligen genomförs en övergripande analys av den utlagda verksamheten i syfte att kunna bedöma behovet av utlagd verksamhet och fånga upp eventuella brister hos tjänsteleverantörer. Detta bedöms nödvändigt för att bibehålla en god intern styrning och kontroll.

		Beredskapsplan.	Rekommendation att Bolaget ser över Bolagets kontinuitetsplan under året 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.
	Klagomålshantering	Interna rutiner och riktlinjer för klagomålshantering.	Ett fåtal rekommendationer kvarstår, vilka lämnats till Bolaget. Se närmare i 2.2 i rapporten.
	IKT-anpassning (avvaktas)	IKT-riktlinje.	Bolaget antog en IKT-riktlinje vid styrelsemötet den 8 juni 2021. Denna kommer att granskas inom ramen för kontroll av Bolagets IKT-anpassning efter att Bolagets granskning av informationssäkerhet och IKT är slutförd och Bolaget erhållit en rapport över granskningen.
	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 nästkommande kvartal.
	IDD	Fortbildningskrav och kunskapstest för anställda som direkt deltar i försäkringsdistribution.	Inga synpunkter.

*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

	Område	*Kontroll*	*Anmärkning*
	N/A		

*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.

Bilaga 2

Nyhetsbrev

23 april 2021

Finansinspektionen beslutar om tillägg till solvenskapitalkravet för Försäkringsbolaget PRI Pensionsgaranti

Finansinspektionen har den 21 april 2021 meddelat beslut om ett tillägg till solvenskapitalkravet (kapitaltillägg) för Försäkringsbolaget PRI Pensionsgaranti, nedan PRI, om 6 251 000 000 kronor. Beloppet är baserat på differensen mellan beräkningen av kapitalkravet enligt standardformel och enligt det modellerade kapitalkrav som Finansinspektionen tagit fram.

PRI har tillstånd av Finansinspektionen att driva direkt och indirekt skadeförsäkringsrörelse i klass 14 (kredit) och direkt skadeförsäkringsrörelse i klass 15 (borgen). PRI driver en försäkringsverksamhet som erbjuder kreditförsäkringar åt företag som har pension i egen regi genom att för sina anställda ta upp pensionsutfästelser som skulder i balansräkningen eller som gör avsättningar till en pensionsstiftelse. Kreditförsäkringen omfattar skadehändelser som t.ex. betalningsinställelse, företagsrekonstruktion och konkurs. PRI är ensamt om att erbjuda denna typ av försäkring på den svenska marknaden.

PRI har beräknat sitt solvenskapitalkrav enligt standardformeln. I beslutet om kapitaltillägg konstaterar Finansinspektionen att PRI:s riskprofil i väsentliga avseenden avviker från de antaganden som ligger till grund för standardformeln. Dessa avvikelser omfattar bl.a. antaganden som ligger till grund för premierisk och kreditfallissemang. Finansinspektionen har också noterat att korrelationen mellan PRI:s marknadsrisk och skadeförsäkringsrisk är betydligt högre än standardformelns korrelation. Detta då 8,8 procent av PRI:s placeringstillgångar är exponerade mot företag som PRI även försäkrar vars konkurs kan ha dubbel påverkan på PRI som kan behöva göra försäkringsutbetalningar samtidigt som PRI:s aktietillgång i det försäkrade företaget går ner i värde.

Om det modellerade kapitalkravet överstiger solvenskapitalkravet enligt standardformeln med mer än 15 procent anses riskprofilen avvika väsentligt från de antaganden som ligger till grund för beräkningen av solvenskapitalkravet enligt standardformeln. Finansinspektionen har tagit fram ett modellerat kapitalkrav för PRI, vilket överstiger kapitalkravet med över 100 procent, och har dragit slutsatsen att avvikelsen är väsentlig och att det därför finns behov av att vidta någon form av korrigerande tillsynsåtgärd.

De korrigerande tillsynsåtgärder som Finansinspektionen kan vidta är att besluta att PRI ska beräkna solvenskapitalkravet med företagsspecifika parametrar alternativt med en intern modell. Om dessa åtgärder bedöms olämpliga kan Finansinspektionen besluta om ett kapitaltillägg.

På grund av att den interna data som PRI har inte bedömts som tillräcklig för att ligga till grund för att beräkna kapitalkravet med företagsspecifika parametrar eller en intern modell samt att arbetet för PRI med att ta fram extern data och expertbedömningar skulle kräva mycket omfattande resurser med osäkert utfall, har Finansinspektionen bedömt att det är olämpligt att besluta att PRI ska beräkna solvenskapitalkravet med företagsspecifika parametrar eller med en intern modell. Finansinspektionen utesluter dock inte att beslut om intern modell kan blir aktuellt framöver.

PRI har uppgett att företaget instämmer i Finansinspektionens bedömning att solvenskapitalkravet beräknat enligt standardformeln inte är rättvisande för PRI:s försäkringsrisk. PRI anser att företagsspecifika parametrar inte är tillämpliga och att det i nuläget inte vore lämpligt att förelägga företaget att utveckla en intern modell. PRI har angett att företaget därför inte har några invändningar i sig mot att Finansinspektionen beslutar om ett kapitaltillägg. PRI har dock framfört ett antal invändningar mot hur Finansinspektionen har beräknat det modellerade kapitalkravet och därmed storleken på ett eventuellt kapitaltillägg. PRI har även invänt mot att kapitaltillägget är väsentligt högre än andra kapitaltillägg som har beslutats inom EU. Vad PRI har invänt har inte motiverat någon annan bedömning från Finansinspektionens sida.

Advokatbyråns rekommendationer

Syftet med solvenskapitalkravet är att försäkringsföretag ska ha tillräckligt med kapital för att kunna absorbera riskerna i hela verksamheten. Advokatbyrån rekommenderar att klienter som lyder under solvensregleringen säkerställer att de antagande som ligger till grund för standardformeln stämmer överens med företagets riskprofil.

Har ni frågor avseende Finansinspektionens beslut eller i övrigt är ni välkomna att kontakta advokatbyrån.

WESSLAU SÖDERQVIST

Nyhetsbrev

11 juni 2021

1 EU-kommissionen har antagit nya standardavtalsklausuler

Enligt EU:s allmänna dataskyddsförordning, nedan GDPR, kan man använda sig av standardavtalsklausuler (*eng*. standard contractual clauses), nedan SCC, godkända av EU-kommissionen för att överföra personuppgifter till ett tredje land. De tre versioner som finns i dagsläget upprättades år 2001, 2004 och 2010 och grundas på det direktiv som gällde innan GDPR trädde i kraft. Mot bakgrund av bl.a. behovet av uppdatering i enlighet med GDPR samt Schrems II-domen[1] har EU-kommissionen den 4 juni 2021 antagit två nya versioner av SCC vilka ersätter de befintliga versionerna. De nya versionerna innebär bl.a. följande;

- Den ena av de två versionerna är tänkt för överföring av personuppgifter inom EU/EES och uppfyller kraven på sådant personuppgiftsbiträdesavtal som krävs enligt GDPR. Personuppgiftsansvariga och personuppgiftsbiträden kan fritt välja att inkludera standardavtalsklausulerna i ett mer omfattande avtal och lägga till andra klausuler eller ytterligare skyddsåtgärder. Detta förutsätter att de inte direkt eller indirekt strider mot SCC eller påverkar de registrerades grundläggande rättigheter och friheter.

- Den andra versionen, avsedd för tredjelandsöverföringar, är mer flexibel än befintliga SCC då den tillhandahåller lämpliga skyddsåtgärder för överföring av personuppgifter från i) personuppgiftsansvarig till personuppgiftsansvarig, ii) personuppgiftsansvarig till personuppgiftsbiträde, iii) personuppgiftsbiträde till personuppgiftsbiträde, och iv) personuppgiftsbiträde till personuppgiftsansvarig. Den nya versionen innebär således att överföringar mellan två personuppgiftsbiträden möjliggörs (vilket ligger utanför tillämpningsområdet för dagens SCC). Detta innebär en möjlighet att täcka situationer där personuppgifter överförs från ett personuppgiftsbiträde inom EU/EES till ett annat personuppgiftsbiträde utanför EU/EES. Den nya versionen tillåter också att fler än två parter ansluter sig till samma avtal. Den nya versionen är därmed mer flexibel än befintliga versioner.

- Särskilda skyddsåtgärder införs i versionen avseende tredjelandsöverföringar mot bakgrund av Schrems II-domen i syfte att hantera eventuella konsekvenser av det mottagande

[1] *Efter den s.k. Schrems II-domen från 2020 har det tydliggjorts att de befintliga standardavtalsklausulerna inte innebär tillräckligt skydd för personuppgifter till ett tredje land. I domen ogiltigförklarade EU-domstolen Privacy Shield som en mekanism för överföring av personuppgifter till USA, men ansåg att SCC fortfarande kan användas. Den personuppgiftsansvarige måste dock göra en undersökning av om lagstiftningen i mottagarlandet säkerställer ett tillräckligt skydd för personuppgifterna innan utkontraktering sker.*

tredjelandets lagstiftning för uppgiftsinförarens efterlevnad av klausulerna, särskilt när det gäller hanteringen av bindande begäran från offentliga myndigheter i det berörda landet om utlämnande av de överförda personuppgifterna.

- Vidare kombineras versionen som avser tredjelandsöverföringar med ett modulärt tillvägagångssätt för att ta hänsyn till olika överföringsscenarier och komplexiteten i behandlingskedjorna. Vid sidan av de allmänna klausulerna bör avtalsparterna välja den modul som är tillämplig i deras situation för att skräddarsy sina skyldigheter enligt SCC i förhållande till sina roller och ansvarsområden.

- Befintliga SCC har tidigare behövt kompletteras med villkor avseende hantering av personuppgiftsincidenter. Detta är nu reglerat i de nya versionerna.

De äldre versionerna av SCC avseende tredjelandsöverföringar som ingåtts före den 27 september 2021 får tillämpas under en övergångsperiod om 18 månader. Avtal med befintliga SCC kan ingås med fortsatt giltighet under en tre månaders övergångsperiod. Detta innebär att avtal som ingåtts på grundval av SCC antagna åren 2001 och 2010 ska anses garantera lämpliga skyddsåtgärder fram till den 27 december 2022. Detta förutsätter att behandlingar som är föremål för avtalet förblir oförändrade. Därefter ska de nya klausulerna ha ingåtts mellan parter där tredjelandsöverföringar av personuppgifter förekommer.

Beslutet för den nya versionen för SCC avseende biträdesavtal inom EU/EES träder i kraft den 27 juni 2021. Det är frivilligt att använda sig av denna version för upprättande av biträdesavtal avseende överföring av personuppgifter inom EU/EES.

2 Wesslau Söderqvist Advokatbyrås synpunkter och rekommendationer

De nya klausulerna ger större flexibilitet då versionen för tredjelandsöverföringar kan tillämpas för flera olika överföringsscenarier och flera parter kan ingå samma avtal. Vidare har det tagits fram en ny version som kan användas som personuppgiftsbiträdesavtal för parter inom EU och som uppfyller kraven på sådant avtal i GDPR. Wesslau Söderqvist Advokatbyrå rekommenderar att de nya klausulerna för tredjelandsöverföring ingås i god tid innan december 2022. För det fall biträdesavtal för överföring av personuppgifter inom EU/EES ska ingås eller ses över rekommenderar Wesslau Söderqvist Advokatbyrå att den nya versionen av SCC tillämpas i syfte att säkerställa att sådant avtal uppfyller de särskilda kraven på biträdesavtal enligt GDPR.

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

WESSLAU SÖDERQVIST

Nyhetsbrev

24 juni 2021

1 Rapport avseende anmälda personuppgiftsincidenter under år 2020

Förra året mottog Integritetsskyddsmyndigheten, nedan IMY, cirka 87 incidentanmälningar i veckan, vilket motsvarar totalt cirka 4 600 personuppgiftsincidenter. Detta är en minskning jämfört med år 2019 då IMY mottog cirka 4 800 anmälningar. I rapporten anges att den vanligaste orsaken till incidenterna har varit den mänskliga faktorn. IMY har publicerat en rapport avseende de inrapporterade personuppgiftsincidenterna och ger däri bl.a. rekommendationer som kan bidra till att förebygga och mildra incidenter. I rapporten anges bl.a. följande.

- En personuppgiftsincident är en säkerhetsincident som omfattar personuppgifter. Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. När en personuppgiftsincident har inträffat ska den personuppgiftsansvarige bedöma vilken risk som incidenten kan medföra. Några faktorer att tänka på är bl.a. typen av incident, personuppgifternas natur, känslighet och volym, hur lätt det är att identifiera enskilda personer samt konsekvensernas svårighetsgrad för enskilda individer. Om det inte är osannolikt att incidenten medför en risk för fysiska personers rättigheter och friheter ska den anmälas till IMY inom 72 timmar från att den upptäckts.

- Av de incidenter som anmäldes år 2020 kom 11 procent från finansiell sektor och den vanligaste incidenten inom denna sektor, liksom för övriga, har varit felaktiga brevutskick. En möjlig förklaring skulle, enligt IMY, kunna vara att det i stor utsträckning skickas personuppgifter per post eller e-post. Jämfört med år 2019 har dock inom finansiell sektor incidenter på grund av obehörig åtkomst minskat med ungefär tio procent. Obehörig åtkomst är dock den näst största kategorin av anmälda personuppgiftsincidenter år 2020 och utgjorde knappt 30 procent av anmälningarna.

- Samtliga organisationer som hanterar personuppgifter behöver ha rutiner för att upptäcka, dokumentera, anmäla och hantera personuppgiftsincidenter. Det behöver även finnas stabila rutiner för att säkerställa att behörigheter tilldelas korrekt, att behörigheterna löpande kontrolleras och följs upp samt att åtkomstkontroller genomförs.

- Den mänskliga faktorn utgör den vanligaste orsaken till anmälda personuppgiftsincidenter. Att största andelen av incidenterna beror på den mänskliga faktorn understryker betydelsen av att styrdokument och tekniska

informationssäkerhetsåtgärder kompletteras med löpande utbildning och andra åtgärder för att öka kunskap och medvetenhet hos medarbetarna. IMY anger att e-posthantering, behov av kryptering av information och förebyggande av antagonistiska angrepp bör ingå i utbildningen.

2 Wesslau Söderqvist Advokatbyrås synpunkter och rekommendationer

Inom finansiell sektor syns en tydlig ökning av incidenter orsakade av mänskliga faktorn. Rekommendationerna som IMY anger är generella. Varje personuppgiftsansvarig måste anpassa sina interna rutiner och riktlinjer för att förhindra personuppgiftsincidenter utifrån den verksamhet som bedrivs. Att rapporten visar på att majoriteten av incidenterna beror på den mänskliga faktorn pekar på viken av att ha tekniska och organisatoriska åtgärder på plats. Wesslau Söderqvist Advokatbyrå rekommenderar även att se över rutiner för tilldelning och översyn av behörigheter i syfte att minska risken för att incidenter inträffar.

Wesslau Söderqvist rekommenderar att översyn av interns rutiner och riktlinjer genomförs på regelbunden basis samt att samtliga anställda inom organisationer som hanterar personuppgifter löpande genomgår för arbetsuppgifterna relevanta utbildningar för att öka kunskapen och medvetenheten inom organisationen.

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

WESSLAU SÖDERQVIST

Nyhetsbrev

24 juni 2021

1 Finansinspektionen meddelar sanktionsbeslut mot Maiden Life AB

Finansinspektionen har meddelat Maiden Life AB, nedan Maiden Life, en varning förenad med sanktionsavgift om 5,5 miljoner kronor. Maiden Life har bl.a. inte uppfyllt kravet på att ha sitt huvudkontor i Sverige, samt vidare inte uppfyllt krav som gäller för outsourcing, oberoende i centrala funktioner, intressekonflikter samt företagsstyrning. Nedan följer några av de överväganden som meddelats i beslutet.

Outsourcing

Maiden Life har lagt ut all sin verksamhet och sina centrala funktioner till tjänsteleverantörer inom och utanför koncernen, bl.a. till ett av sina systerbolag. Maiden Life omfattas således av krav på dels uppdragsavtal, dels skriftliga styrdokument för utlagd verksamhet som bl.a. omfattar Maiden Lifes övervakningsrutiner avseende den utlagda verksamheten. Maiden Lifes styrdokument är på en mycket övergripande nivå och saknar information om vilka faktiska övervakningsrutiner som ska tillämpas vid övervakningen. Enbart en upplysning om att det ska finnas en process för övervakning, att styrelsen regelbundet ska bedöma arrangemanget och att en granskningsprocess ska inrättas räcker enligt Finansinspektionen inte för att styrdokumentet ska anses innehålla rutiner i den mening som krävs enligt gällande lagstiftning.

Uppdragsavtal avseende kritiska eller viktiga operativa funktioner eller verksamheter omfattas av ett antal krav på innehåll. Det ställs bl.a. krav på att tjänsteleverantören ska iaktta Maiden Lifes styrdokument, samarbeta med tillsynsmyndigheter samt omfattas av krav på informationsplikt och att revisorer, liksom tillsynsmyndigheter, ska ges tillgång till lokaler och information. Några sådana krav har inte funnits i Maiden Lifes uppdragsavtal med systerbolaget.

Något utrymme att mildra kraven för Maiden Life i dessa delar med hänvisning till proportionalitetsprincipen har inte funnits.

Oberoende i centrala funktioner

En av styrelseledamöterna i Maiden Life har varit ansvarig för bolagets funktion för regelefterlevnad, nedan funktionsansvarig, och utfört arbete i funktionen. Den funktionsansvarige, som även är anställd i systerbolaget, har utfört ett flertal arbetsuppgifter i den operativa verksamheten, bl.a. arbete hänförligt till reservsättning, ORSA[1] och förberedande

[1] *Bolagets egna risk- och solvensbedömning.*

av data till solvenskapitalberäkningar. Den funktionsansvarige har dessutom ingått i riskhanteringsfunktionen samt i aktuariefunktionen och i denna roll upprättat rapporter till Maiden Lifes styrelse. Finansinspektionen konstaterar att den funktionsansvarige har utfört ett stort antal uppgifter i den verksamhet, och även i andra centrala funktioner, som personen har haft i uppdrag att kontrollera. Dessutom har den funktionsansvarige granskat områden där personen själv har varit operativt verksam.

Finansinspektionen bedömer vidare att samtliga personer i Maiden Lifes riskhanteringsfunktion, i sina roller i den operativa verksamheten, har haft uppgifter som har en direkt påverkan på såväl riskprofilen som riskhanteringssystemet. Eftersom det ingår i riskhanteringsfunktionens uppgifter att övervaka riskprofilen och riskhanteringssystemet på ett objektivt och oberoende sätt, anser Finansinspektionen att det inte för någon av de personer som har ingått i riskhanteringsfunktionen har funnits förutsättningar för sådan övervakning. Intressekonflikter inom funktionen har således, till skillnad från vad bolaget hävdar, inte ens varit möjliga att hantera.

Intressekonflikter

Maiden Life och systerbolaget har finansiella förbindelser som utgör en potentiell källa till intressekonflikter eftersom större delen av Maidens Lifes verksamhet är utlagd till systerbolaget. Finansinspektionen har bl.a. konstaterat att intressekonflikter förelegat när Maiden Lifes styrelseordförande ansvarat för systerbolagets leverans av försäkringsrelaterade och administrativa tjänster till Maiden Life, samtidigt som han varit ytterst ansvarig i Maiden Life för att utvärdera leveransen enligt uppdragsavtal. Även det faktum att två av styrelseledamöterna samtidigt har ansvarat för centrala funktioner och utfört stora delar av arbetet i funktionerna ger enligt Finansinspektionen upphov till intressekonflikter. Det har dessutom i styrelseprotokoll gått att utläsa att de inte på något sätt har haft en intressekonflikt i förhållande till någon av mötespunkterna.

Företagsstyrning

Bestämmelser om företagsstyrning omfattas av proportionalitetsprincipen. Finansinspektionen understryker i beslutet att principen inte ska tolkas som att alla krav kan ändra innebörd genom ett sådant beaktande. Än mindre kan det betyda att något krav bortfaller. Finansinspektionen anser inte att Maiden Life, vilket de själva hävdade, kunde anses uppfylla samtliga krav avseende företagsstyrning med tillämpning av proportionalitetsprincipen.

Maiden Life har brustit i sin regelefterlevnad genom att inte uppfylla krav som gäller outsourcing, centrala funktioners oberoende och intressekonflikter. Överträdelserna rör bestämmelser som är centrala för en fungerande företagsstyrning. Det innebär enligt

Finansinspektionen att Maiden Life, genom dessa överträdelser, inte har uppfyllt kravet på att ha en sund och ansvarsfull företagsstyrning.

Överväganden vid beslut

Det har i flera fall varit fråga om allvarliga överträdelser som har pågått under lång tid. Mot bakgrund av att Maiden Life har vidtagit åtgärder för att rätta till brister och gjort förändringar i bolagets styrelse och ledning samt att Finansinspektionen gjort bedömningen att överträdelserna inte kommer att upprepas, har bolaget meddelats en varning förenad med sanktionsavgift på 5,5 miljoner kronor.

2 Wesslau Söderqvist Advokatbyrås synpunkter och rekommendationer

Maiden Life har tillstånd av Finansinspektionen att driva försäkringsrörelse enligt försäkringsrörelselagen. Slutsatser som går att dra av beslutet och Finansinspektionens överväganden bedöms dock kunna vara av relevans även för samtliga tillståndspliktiga företag som omfattas av regler avseende outsourcing, intressekonflikter, oberoende i centrala funktioner och intern styrning och kontroll. Mot bakgrund av detta rekommenderar Wesslau Söderqvist att sanktionsbeslutet bör läsas i sin helhet. I beslutet ges även ledning kring tolkning och tillämpning av proportionalitetsprincipen.

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