Göteborgs Stad

Tjänsteutlåtande
Utfärdat 2019-01-22
Diarienummer 0035/18

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

Punkt 17 Rapport Regelefterlevnadsfunktionen kvartal 4 2018

Förslag till beslut i styrelsen för Försäkrings AB Göta Lejon

- anta Rapporten Regelefterlevnadsfunktionen kvartal 4 2018

Sammanfattning

Regelefterlevnadsfunktionen ska årligen tillhandahålla styrelsen en skriftlig sammanställning av föregående års arbete.

Ekonomiska konsekvenser

Bolaget har inte funnit några särskilda aspekter på frågan utifrån detta perspektiv.

Barnperspektivet

Bolaget har inte funnit några särskilda aspekter på frågan utifrån detta perspektiv.

Mångfaldsperspektivet

Bolaget har inte funnit några särskilda aspekter på frågan utifrån detta perspektiv.

Jämställdhetsperspektivet

Bolaget har inte funnit några särskilda aspekter på frågan utifrån detta perspektiv.

Miljöperspektivet

Bolaget har inte funnit några särskilda aspekter på frågan utifrån detta perspektiv.

Omvärldsperspektivet

Bolaget har inte funnit några särskilda aspekter på frågan utifrån detta perspektiv.

Bilagor

1. Årsrapport Regelefterlevnadsfunktionen 2018

Ärendet

Beskrivning av ärendet

Regelefterlevnadsfunktionen har i enlighet med granskningsplanen gjort en sammanställning av 2018 års rekommendationer och en statusuppdatering

Bolagets bedömning

Det är bolagets bedömning att rekommendationerna är rimliga och att bolaget kommer att kunna åtgärda dessa med befintliga resureser.

Katrin Gundersen	Annika Forsgren
Bolagsjurist	VD

Försäkrings AB Göta Lejon

Compliancerapport
Kvartal 4 2018

Empower Results®

Innehållsförteckning

Inledning

Bakgrund

Styrelsen ansvarar för att en god intern kontroll präglar organisationen och driften av bolaget och se till att det finns en funktion (compliance) som utgör ett stöd för att verksamheten drivs enligt gällande regler.

Aon Global Risk Consulting AB (compliancefunktionen) har fått i uppdrag att följa upp Försäkrings AB Göta Lejon (bolaget) regelefterlevnad och avrapportera eventuella avvikelser utifrån krav på interna riktlinjer till följd av lag eller riktlinje/allmänt råd utfärdat av FI, EIOPA och Solvens II-direktiv.

Syfte

Compliancefunktionen har granskat Försäkrings AB Göta Lejon (bolaget) regelefterlevnad i enlighet med gällande granskningsplan för 2018-2020.

För granskning fjärde kvartalet ingår:

- Revisionsutskott – Granskning och utvärdering av bolagets rutiner för Revisionsutskottet.
- Personuppgiftslagen (GDPR) - Kontroll av att rutiner och systemförteckningar finns på plats och efterföljs.

Regelverk

Följande regelverk har legat till grund för denna granskning:

- Aktiebolagslagen 2005:551
- Försäkringsrörelselagen 2010:2043
- Europaparlamentet och rådets förordning EU 2016/679

Kontakt

Funktionen har inhämtat information från följande personer:

Ekonomichef, Björn Wennerström och Bolagsjurist, Katrin Gundersen.

Undertecknad reserverar sig för ev. sakfel pga. inkorrekt och/eller avsaknadinformation.

Genomförd granskning enligt plan

Uppföljning av tidigare rekommendationer

Bedömning	**Förmånsrättsregister** FTA och främst beräkningen av bästa skattning plus en riskmarginal bör uppdateras kvartalsvis i samband med beräkning för QRT så att samma värde användas i förmånsrättsregistret. Bolagets åtgärd: Registeransvarig uppdaterar förmånsrättsregistrets beräkning av FTA samt bästa skattning plus riskmarginal till det värde som räknas fram för kvartalsvisa QRT rapporten. **Bolagets rutiner för placering av tillgångar** Bolagets dokument Finansiell anvisning, hänvisar till rättslig grund EIOPA_CP_ 13/08 Riktlinje 31 vilken har utgått och ersatts med EIOPA BoS-14/253 riktlinje 29 och 36. Bolagets åtgärd: Uppdatera rättslig grund i dokumentet Finansiell anvisning till EIOPA BoS-14/253 riktlinje 29 och 36.
Rekommenderad åtgärd	Inga ytterligare.

Granskning och utvärdering av bolagets rutiner för revisionsutskottet

Bedömning	<u>Krav enligt 8 kap. 49b ABL</u> *Revisionsutskottet ska, utan att det påverkar styrelsens ansvar och uppgifter i övrigt:* *1. övervaka bolagets finansiella rapportering samt lämna rekommendationer och förslag för att säkerställa rapporteringens tillförlitlighet,* *2. med avseende på den finansiella rapporteringen övervaka effektiviteten i bolagets interna kontroll, internrevision och riskhantering,* *3. hålla sig informerat om revisionen av årsredovisningen och koncernredovisningen samt om slutsatserna av Revisorsinspektionens kvalitetskontroll,* *4. informera styrelsen om resultatet av revisionen och om på vilket sätt revisionen bidrog till den finansiella rapporteringens tillförlitlighet samt om vilken funktion utskottet har haft,* *5. granska och övervaka revisorns opartiskhet och självständighet och då särskilt uppmärksamma om revisorn tillhandahåller bolaget andra tjänster än revision.* *6. biträda vid upprättandet av förslag till bolagsstämmans beslut om revisorsval.* **Iakttagelser rutin:** Bolagets har beslutat att inte införa ett särskilt revisionsutskott, utan styrelsen gemensamt utgör- och utför de arbetsuppgifter som annars skulle falla under revisionsutskottet. Revisionsutskottet tillika styrelsen har genomgått informationsutbildning genomförd av EY för vilka uppgifter- samt hur dessa kan utföras av styrelsen. Revisionsutskottet avger en rapport baserat på ovan uppgifter och krav vilken behandlades på styrelsemötet nr 2 den 9 februari 2018. Beslut fattade av styrelsen genom revisionsutskottet noteras i ordinarie styrelseprotokoll. Compliancefunktionen anser att ovan punkter har behandlats under året med stöd av styrelse-protokollen och revisionsutskottets rapport. Dock saknas det angivelse i styrelsens arbetsordning att ovan uppgifter ska behandlas och att styrelsen gemensamt utgör bolagets revisionsutskott.
Rekommenderad åtgärd	I riktlinjen för styrelsens arbetsordning ange att styrelsen även utgör och utför revisionsutskottets ansvar och uppgifter.

Granskning och utvärdering av bolagets rutiner och systemförteckning enligt GDPR

Bedömning	Undertecknad har utfört stickprovskontroller avseende följande områden: 1) Kunskap och medvetenhet om GDPR i organisationen ➢ punkten har behandlats genom b.la internutbildning. Viktigt är att ha utbildningsrutiner för nyanställda. 2) Internt regelverk för hantering av personuppgifter enligt GDPR ➢ ett flertal riktlinjer har upprättats och godkänts av styrelsen b.la hantering av e-post, fritextfält och riktlinjer för hantering av personuppgifter i Göteborgs Stad. ➢ Kvarstår att upprätta instruktioner för hantering av ostrukturerat material, begäran om rättning och eller radering av uppgifter, rutiner för hantering av personuppgifteincident och begäran utav registerutdrag. 3) Registerförteckning (register över aktuell personuppgiftsbehandling) ➢ se nedan. 4) Personuppgiftsbiträdesavtal för att säkerställa krav mot personuppgiftsbiträden ➢ bolaget har inventerat och upprättat personuppgiftsbiträdesavtal för samarbetspartners 5) Information till registrerade (kunder) ➢ Viss uppdatering av informationstext till berörda har upprättats, dock kvarstår kompletteringsarbete i blanketter etc. Punkten hanteras gemensamt med bolagets DSO. 6) Dataportabilitet ➢ Det är i dagsläget inte klart hur rätten till dataportabilitet ska hanteras systemmässigt. Frågan avser överföring av information i situationer där uppgifter lämnats av den registrerade enligt lagliga grunderna samtycke eller fullgörande av avtal och finns vidare beskrivet i artikel 20. 7) Rutin för registerutdrag ➢ Interna rutiner och hantering av begäran om registerutdrag saknas. Punkten kvarstår att hantera i enlighet med artikel 15. 8) Dataskyddsombud (DSO) ➢ Dedikerat dataskyddsombud för Göta Lejon finns utsett inom staden. 9) Anmälan av personuppgiftsincidenter samt information till registrerad i vissa fall

	➢ Rutiner och instruktioner för hantering av personuppgifteincidenter kvarstår att upprätta i enlighet med artikel 33 och 34. 10) konsekvensbedömning avseende dataskydd (vid behandling som sannolikt leder till hög risk för den registrerade) ➢ Rutiner och instruktioner saknas idag för att bedöma konsekvenser vid nya behandlingar. Oklart om tex DSO har system eller verktyg för att utföra DPIA (Data Privacy Impact Assessment) enligt artikel 35. **3) Registerförteckning** Förutsättningar utifrån artikel 30: Både personuppgiftsansvarig och personuppgiftsbiträde ansvarar för att upprätta en registerförteckning i enlighet med angivna krav. Förteckningen ska innehålla bl.a. - ändamålen med behandlingen, - en beskrivning av kategorierna av registrerade samt kategorierna av personuppgifter, - kategorier av mottagare inkl. mottagare i tredje land - tidsfrist för radering - om möjligt tekniska och organisatoriska säkerhetsåtgärder enligt artikel 32.1. **Iakttagelser och rutin:** Nuvarande registerförteckning, (Excell dokument för migrering av personuppgifter), är anpassad till kommunens verksamhet vilket i sig är ändamålsenligt dock saknas en del information vilket gör registret inkomplett och inte helt anpassat enligt kraven i GDPR. t.ex. saknas uppgift om personuppgiftsbiträde, tidsfrist för radering och tekniska och organisatoriska säkerhetsåtgärder (loggning, kryptering, behörighetsstyrning m.m.). Delar av den avsaknad information återfinns dock i GAP-analysens Excel register. Göteborgs Stad kommer att införa ett digitalt system för förande av personuppgiftsbehandlingar och förväntas finnas på plats under februari 2019, vilket troligen löser problematiken.
Rekommenderad åtgärd	I avvaktan på digitalt system kan befintligt Excelregister kompletteras med uppgift om personuppgiftsbiträde, tidsfrist för radering och om möjligt tekniska och organisatoriska säkerhetsåtgärder. Viktigt är också att utforma rutiner för hur nya behandlingar ska införlivas i registret.

Omvärldsbevakning

Uppdatering av diskonteringsräntekurvor

Finansinspektionen publicerar nya diskonteringsräntekurvor, för december 2018, tisdagen 8 januari 2019.

Här publiceras diskonteringsräntekurvor.

FI granskar försäkringsföretags hantering av förmånsrättsregister

Finansinspektionen har beslutat att starta en undersökning kring försäkringsföretagens hantering av förmånsrättsregister. Syftet är att undersöka företagens processer för hur de arbetar med registren. När ett försäkringsföretag går i konkurs innebär att det finns en prioritetsordning som ger försäkringstagare och andra ersättningsberättigade särskild förmånsrätt.
Inom ramen för denna modell ska försäkringsföretagen upprätta ett register med tillgångar som ska omfattas av den särskilda förmånsrätten, ett så kallat förmånsrättsregister. Detta ska göras i enlighet med 6 kap. 11 § i försäkringsrörelselagen och registrets utformning framgår av FFFS 2015:8 5 kap.

Undersökningen riktas till ett urval av försäkringsföretag. De kommer att få en enkät som handlar om hur de hanterar förmånsrättsregistret. Undersökningens resultat kommer presenteras i en rapport under våren 2019

Rapporter från tillsynsmyndigheten – Finansinspektionen

Digitaliseringen i den finansiella sektorn ökar samtidigt som nya innovationer skapar produkter, affärsmodeller och samarbetsformer som ställer högre krav på riskhantering, styrning och kontroll av IT-verksamheten än tidigare. Detta gäller särskilt styrning och kontroll av IT-verksamhet som omfattas av uppdragsavtal eftersom utlagd verksamhet inte är lika transparent som när den drivs i egen regi.

Samtidigt kan utläggning av IT-verksamheten leda till både kvalitetshöjningar och besparingar. Nya eller små aktörer inom försäkring kan med moderna och jämförelsevis billiga tjänster från professionella IT-leverantörer konkurrera på marknader som de annars inte skulle haft tillgång till.

Omfattningen av uppdragsavtal kan i hög grad påverka ett försäkringsföretags förmåga att överblicka och hantera konsekvenserna av sina it-strategiska vägval.

Vad gäller de strategiska vägval ett försäkringsföretag gör för IT-verksamheten lägger FI stor vikt vid följande frågeställningar:

- Hur avgör företaget att verksamhetens system, resurser och rutiner är lämpliga i förhållande till verksamhetens kontinuitetskrav?
- Hur identifierar och värderar företaget risker i IT-verksamheten i förhållande till andra strategiska risker som it-riskerna påverkar:
    - o i samband med förändringar av företagets affärsstrategi?
    - o i större projekt och investeringar?

- Hur identifieras, bedöms och hanteras nya it-behov i förhållande till verksamhetens övergripande affärsmål?

Även om rapporten tar sikte på nya innovativa försäkringsprodukter och nya tekniska möjligheter finns ett särskilt fokus på utlagd verksamhet. Och Finansinspektionen påpekar att uppdragsavtal inte inskränker på ett försäkringsföretags ansvar och att kvaliteten i försäkringsföretagets företagsstyrningssystem inte får försämras väsentligt vid utlagd verksamhet. Ett försäkringsföretag måste kunna visa att styrning och bevakning av IT-verksamheten är ändamålsenlig och hur verksamheten uppfyller kraven på riskhantering.

Åtgärd/påverkan Göta Lejon:
Även om bolaget har styrdokument avseende uppdragsavtal i enlighet med de regulatoriska kraven samt en väl utvecklad process för utvärdering av uppdragstagare, som främst tar sikte externa uppdragstagare, finns härav anledning för bolaget att överväga samma utvärderingsprocedur för den gruppinterna IT supporten och tex Insman.
Och i bolagets egna riskregister beakta/utvärdera cyberrisker som ett led att stärka riskhantering.

Kontaktuppgifter

Stockholm 2018-12-21

_____

Stefan Hederstedt
Compliance
För Aon Global Risk Consulting AB

Josefine Dawson

Compliance Officer

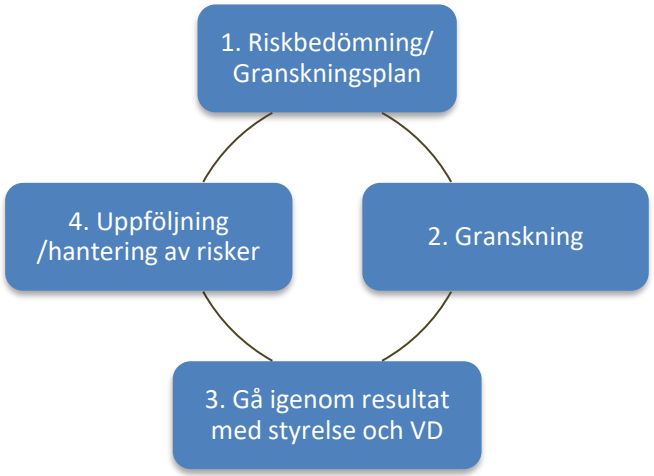
Aon Global Risk Consulting AB

+46 76 002 45 70

josefine.dawson@aon.se

Riskgradering och arbetsmetodik

Risk	Rekommenderad åtgärd
	Risken/regelöverträdelsen är av betydande art och bolaget bör omedelbart vidta åtgärder för att minimera/åtgärda risken/regelöverträdelsen.
	Risken/regelöverträdelsen är av mindre art och bolaget bör vid tillfälle vidta åtgärder för att minimera/åtgärda risken/regelöverträdelsen.
	Det granskade området följer gällande regler. Inga åtgärder måste vidtas.



Compliance funktionens uppdrag är utlagd via uppdragsavtal till Aon Global Risk Consulting och resulterar i flera granskningsrapporter och är likväl en stödresurs under hela året avseende frågeställningar och support samt utbildning via avropat från bolagets ledning