3. nóvember 2021
Tilvísun: 2106077

Dreifibréf númer: 62/2021
til vátryggingafélaga og Samtaka fjármálafyrirtækja

Efni: Viðmiðunarreglur EIOPA um áhættu og öryggi vegna upplýsinga- og samskiptatækni og stjórnarhætti þeim tengdum.

Evrópska vátrygginga- og lífeyrissjóðaeftirlitsstofnunin (EIOPA) hefur gefið út viðmiðunarreglur (e. guidelines) um upplýsingatækni og netnotkun[1] (e. ICT, hér eftir UST) vegna upplýsinga- og samskiptatækni og stjórnarhætti þeim tengdum (EIOPA-BoS-20-600).

Viðmiðunarreglurnar, sem eru 25 talsins, taka til upplýsingatækni og öryggis og stjórnarhátta þeim tengdum, líkt og leiðbeinandi tilmæli (LT) Fjármálaeftirlits Seðlabanka Íslands (hér eftir Fjármálaeftirlitið), vegna áhættu við rekstur upplýsingakerfa eftirlitskyldra aðila nr. 1/2019. Fjármálaeftirlitið beinir því til vátryggingafélaga að kynna sér viðmiðunarreglurnar, sem aðgengilegar eru á heimasíðu Seðlabankans, og taka framvegis mið af þeim í starfsemi sinni m.t.t. áhættu og öryggis vegna upplýsinga- og samskiptatækni og stjórnarhátta þeim tengdum. Vakin er athygli á því að það eru ákveðin atriði í EIOPA viðmiðunarreglunum sem eru ítarlegri en í LT nr. 1/2019. Má þar einkum nefna eftirfarandi:

- Eftirlitsskyldum aðila ber að kortleggja og framkvæma mat og prófanir á öryggi upplýsinga með ítarlegri hætti en hingað til hefur verið gerð krafa til (viðmiðunarreglur 11 og 12).
- Gerðar eru meiri kröfur til þekkingar, þjálfunar og meðvitundar um upplýsingaöryggi starfsmanna eftirlitsskyldra aðila og er sérstaklega tekið fram að slíkt eigi einnig við um stjórnendur og stjórn (viðmiðunarreglur 13).
- Eftirlitsskyldur aðili skal skilgreina, skjalfesta og útfæra málsmeðferð fyrir aðgang í samræmi við kröfur um vernd eins og þær eru skilgreindar í viðmiðunarreglu 4. Slíkar verklagsreglur þurfa að lágmarki að uppfylla ákveðin skilyrði skv. tölulið 26 a-i viðmiðunarreglu 8.
- Gerðar eru kröfur um áþreifanlegar öryggisráðstafanir félaga (t.d. vernd gegn tjóni af völdum rafmagnsleysis, elds, vatns og óviðkomandi aðgangs í húsnæði/tækjum), þ.m.t. að skilgreina, skjalfesta og útfæra ráðstafanir til að vernda húsnæði, gagnaver og viðkvæm svæði fyrir óheimilum aðgangi og frá

[1] Varðandi samskipta- og/eða netnotkunarhlutann (e. communications), þá fellur hluti hans undir tilmæli um skýjaþjónustuveitendur (e. Guidelines on Outsourcing to Cloud Service Providers EIOPA-BoS-20-002). Samkvæmt skilgreiningu á það bæði við um „software og hardware" notkun á netinu og í skýinu.

umhverfisáhættu. Hér undir fellur einnig krafa um að aðgangur að UST-kerfum sé aðeins leyfður fyrir ákveðna einstaklinga. Heimild skal úthlutað í samræmi við verkefni aðila og ábyrgð og ætti hún að takmarkast við einstaklinga sem eru þjálfaðir á viðeigandi hátt. Þá þarf að rýna og vakta aðganginn og endurskoða aðgengi að honum reglulega til að tryggja það að strax sé lokað fyrir óþarfa aðgangsrétt (viðmiðunarregla 9).

- Eftirlitsskyldur aðili á að halda uppfærða skrá yfir UST-eignir sínar, og skal skráin vera nægilega ítarleg til að hægt sé að bera auðveldlega kennsl á UST-eignir, staðsetningu, öryggisflokkun og eignarhald félagsins (viðmiðunarregla 14).
- Þá er fjallað um viðbúnaðar – og viðreisnaráætlanir, viðbrögð, rekstrarsamfellu, krísusamskipti, prófanir o.fl. (viðmiðunarreglur 20-24).

Viðmiðunarreglurnar útfæra nánar ákvæði 41., 44., 46., 47., 132. og 246. tilskipunar 2009/138/EB (Solvency II tilskipunin), sbr. 39., 44., 46., 47. og 113. gr. laga nr. 100/2016 um vátryggingastarfsemi, sbr. og til hliðsjónar 37. gr. sömu laga, og ákvæði 258. til 260., 266., 268. til 271. og 274. gr. framseldrar reglugerðar (ESB) 2015/35 um viðbætur við Solvency II tilskipunina, sbr. a. lið 2. gr. reglugerðar nr. 940/2018, um gildistöku reglugerða Evrópusambandsins um vátryggingastarfsemi og vátryggingasamstæður. Jafnframt byggja viðmiðunarreglurnar á ákvæðum viðmiðunarreglna EIOPA um útvistun til skýjaþjónustuaðila (EIOPA-BoS-20-002) og viðmiðunarreglum EIOPA um stjórnkerfi vátryggingafélaga (EIOPA-BoS-14/253).

Viðmiðunarreglur EIOPA-BoS-20-600 tóku gildi 1. júlí 2021 innan Evrópusambandsins og eru aðgengilegar hér.

Samkvæmt 3. mgr. 16. gr. ESAs reglugerðanna, sem innleiddar voru með lögum nr. 24/2017 um evrópskt eftirlitskerfi á fjármálamarkaði, eiga lögbær yfirvöld og viðkomandi eftirlitsskyldir aðilar að leita allra leiða til að fara að viðmiðunarreglum eftirlitsstofnananna og almennum tilmælum. Tilgangur viðmiðunarreglnanna er að koma á samhæfðri, skilvirkri og árangursríkri eftirlitsframkvæmd innan evrópska fjármálakerfisins og tryggja sameiginlega, einsleita og samræmda beitingu á löggjöf innan EES.

Með vísan til framangreinds ber vátryggingafélögum að kynna sér framangreindar viðmiðunarreglur EIOPA og taka framvegis mið af þeim í starfsemi sinni. Fjármálaeftirlitið mun samhliða styðjast við viðmiðunarreglur EIOPA við mat á því hvort vátryggingafélög uppfylli kröfur samkvæmt þeim ákvæðum í lögum og tilmælum sem fjallað er um í þessu dreifibréfi.

Virðingarfyllst,

SEÐLABANKI ÍSLANDS

Rúnar Guðmundsson
framkvæmdastjóri
lífeyris og vátrygginga

Sigurveig Guðmundsdóttir
sérfr. í áhættugreiningu
lífeyris og vátrygginga