3. nóvember 2021
Tilv.: 2106077

Dreifibréf númer: 63/2021
til lífeyrissjóða og Landssamtaka lífeyrissjóða

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 upplýsingatæknimála 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. Þar sem umræddar viðmiðunarreglur eru ítarefni við LT nr. 1/2019, beinir Fjármálaeftirlitið því til lífeyrissjóða að kynna sér viðmiðunarreglurnar, sem aðgengilegar eru á heimasíðu Seðlabankans, og taka framvegis mið af þeim við rekstur þeirra upplýsingakerfa sem þýðingu hafa fyrir eða áhrif á starfsemi þeirra.

Vakin er athygli á því að ákveðin atriði í EIOPA viðmiðunarreglunum 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

[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.

vernda húsnæði, gagnaver og viðkvæm svæði fyrir óheimilum aðgangi og frá 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).
- Fjallað er um viðbúnaðar– og viðreisnaráætlanir, viðbrögð, rekstrarsamfellu, krísusamskipti, prófanir o.fl. (viðmiðunarreglur 20-24).

Viðmiðunarreglur EIOPA-BoS-20-600 tóku gildi 1. júlí 2021 á Evrópska efnahagssvæðinu 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 viðmiðunarreglna EIOPA er að koma á samhæfðri, skilvirkri og árangursríkri eftirlitsframkvæmd innan evrópska fjármálakerfisins og tryggja sameiginlega, einsleita og samræmda beitingu á löggjöf innan EES.

Fjármálaeftirlitið mælist til þess að lífeyrissjóðir kynni sér framangreindar viðmiðunarreglur EIOPA á vefsíðu Seðlabankans og taki framvegis mið af þeim í starfsemi sinni við rekstur þeirra upplýsingakerfa sem hafa þýðingu fyrir eða áhrif á starfsemina. Fjármálaeftirlitið mun styðjast við viðmiðunarreglurnar við mat á því hvort ákvæði LT nr. 1/2019 séu uppfyllt.

Virðingarfyllst,
SEÐLABANKI ÍSLANDS

Rúnar Guðmundsson
framkvæmdastjóri
lífeyris og vátrygginga

Sigurveig Guðmundsdóttir
sérfr. í áhættugreiningu
lífeyris og vátrygginga