FJÁRMÁLAEFTIRLITIÐ
THE FINANCIAL SUPERVISORY AUTHORITY, ICELAND

Samantekt umsagna vegna umræðuskjals nr. 3/2014

Umsagnir bárust frá eftirtöldum aðilum:

1. Arion banka hf.
2. Borgun hf.
3. Lýsingu hf.
4. Viðlagatryggingum Íslands

Umsagnir aðila sem óska eftir trúnaði er ekki að finna í þessari samantekt. Umræðuskjal nr. 3/2014 varð að leiðbeinandi tilmælum nr. 2/2014 um upplýsingakerfi eftirlitsskyldra aðila

Nr.	Nafn umsagnaraðila	Tilvísun	Umsögn
1.	Viðlagatrygging Íslands	Almenn athugasemd	Staðfestir Viðlagatrygging að umræddar breytingar séu allar til bóta
2.	Arion banki hf.	Almenn athugasemd	I. Almennt Arion banki hf. (hér eftir Arion banki eða bankinn) vísar til dreifibréfs og umræðuskjals Fjármálaeftirlitsins sem barst bankanum þann 28. janúar sl., um endurskoðun leiðbeinandi tilmæla um upplýsingakerfi eftirlitsskyldra aðila. Þakkar Arion banki það tækifæri að fá að koma á framfæri athugasemdum og ábendingum varðandi tilmælin. Í dreifibréfinu kemur fram að með endurskoðun tilmælanna sé brugðist við athugasemdum sem Fjármálaeftirlitinu hafa borist eftir að tilmælin tóku gildi og varði þær einkum skýrleika þeirra. Til viðbótar kemur fram að aðeins sé óskað eftir umsögn við þá liði tilmælanna sem hefur verið breytt. Arion banki telur nauðsynlegt að nefna nokkra þætti sem ekki hefur verið breytt frá upphaflegum tilmælum, m.a. þar sem bankinn hefur áður komið þeim á framfæri við Fjármálaeftirlitið. II. Dreifibréf FME dags. 10. október sl. Arion banki vísar til dreifibréfs Fjármálaeftirlitsins sem sent var bankanum á haustdögum, „Breyting á skilaeindegi vegna áhættugreiningar upplýsingatækni“ og þeim samskiptum sem bankinn átti við eftirlitið í kjölfar þess, m.a. tölvupóstsamskipti 11., 14., 15. og 23. október sl. og fund þann 21. október sl. Með dreifibréfinu og svari eftirlitsins í fyrrgreindum samskiptum kom fram að i) hafi ákveðnum skilaeindaga verið frestað og ii) áhættugreiningu verði ekki skilað til Fjármálaeftirlitsins eins og fram kom í tilmælunum. Arion banki ítrekar að þessi framkvæmd eftirlitsins var óheppileg. Sérstaklega þar sem dreifibréfið barst þann 10. október, þegar um þrjár vikur voru í skil á áhættumati bankans. Mikil og kostnaðarsöm vinna hafði farið fram innan bankans sem miðaði að því að tekið væri tillit til þess að skil væru fyrir lok október sl. Það var því óþægilegt að skilum væri frestað og framkvæmd breytt með stuttum fyrirvara á eins nýjum tilmælum og um var að ræða. Það er því von Arion banka að hægt verði að treysta þeirri framkvæmd sem hin nýju tilmæli kveða á um. III. Tenglar á vefsíður Arion banki bendir Fjármálaeftirlitinu á að svo virðist sem þær vefsíður sem vísað er til í neðanmálsgrein tvö virki ekki, eða séu beint inn á tilteknar vefsíður, án þess að vísað sé til

			tiltekinna reglna eða tilmæla. IV. Notkun tiltekinna hugtaka í tilmælunum Arion banki telur rétt að nefna notkun nokkurra hugtaka í tilmælunum, þá sérstaklega í 9. kafla þeirra. Það er ekki alveg ljóst hvort hugtökin viðskiptafyrirmæli og viðskiptaupplýsingar samkvæmt tilmælunum séu í einhverjum tilvikum ætlað að hafa sömu merkingu. Þrátt fyrir að leitast sé nú við að skilgreina viðskiptaupplýsingar. Auk þessa er ekki ljóst hvort með hugtakinu viðskiptafyrirmæli sé vísað til viðskiptafyrirmæla skv. lögum nr. 108/2007, um veðbréfaviðskipti. Til viðbótar er þarft að nefna nokkur atriði varðandi einstaka liði innan 9. kafla tilmælanna og útskýra betur: • Grein 9.2.3 kveður á um að afrit af upplýsingakerfum sem innihalda viðskiptaupplýsingar séu tiltæk að lágmarki í tvö ár frá uppruna skráningar. • Grein 9.2.4 fjallar síðan um afrit af upplýsingakerfum sem innhalda viðskiptafyrirmæli séu tiltæk frá uppruna skráningar. • Grein 9.2.5 kveður á um tímamörk í samræmi við lög um bókhald. o Grein 9.3. kemur inn á að „ofangreind“ kerfi falla öll þau upplýsingakerfi eftirlitsaðila sem innhalda skráningar og gögn sem varða viðskipta- og fjárhagsupplýsingar. Enn fremur er hér einnig átt við öll upplýsinga- og samskiptakerfi er tengjast viðskiptum, s.s. tölvupóstur, símkerfi, farsímar, föx snarspjall eða annarskonar samskiptakerfi, auk annarra gagna sem innhalda viðskiptafyrirmæli. o Grein 9.3.1. útskýrir upp að ákveðnu marki hvað eru viðskiptafyrirmæli. o Grein 9.2.3. fjallar nánar um viðskiptafyrirmæli. Í fyrsta lagi þá er ekki ljóst hvað nákvæmlega fellur undir viðskiptaupplýsingar, enda kemur hugtakið sem slíkt ekki fram í lögum á fjármálamarkaði, öðrum en lögum um kauphallir (ekki skilgreiningu að finna þar) og ekki er útskýrt í tilmælunum hvað nákvæmlega fellur þar undir, sbr. t.d. 9.2.3. Í neðanmálsgrein þrjú í drögum að nýjum tilmælum er þó leitast við að skilgreina „viðskiptaupplýsingar“, þar kemur fram að með viðskiptaupplýsingum sé átt við allar upplýsingar og gögn um viðskiptavini og stöðu hans gagnvart viðkomandi eftirlitsskyldum aðila. Arion banki telur að þessi skilgreining sé of víðtæk og erfitt að átta sig á hvar mörkin liggja. Í öðru lagi, þá er ekki fyllilega ljóst hvernig skilja megi grein 9.2.3. þar sem 9.3.1 og 9.2.3 [sem] kemur beint á eftir á við um viðskiptafyrirmæli og þykir því óskýrt hvort grein 9.3. eigi aðeins við um slíkar upplýsingar eða ekki. Greinina má skýra víðtækara miðað við þau hugtök sem í henni eru notuð. Til viðbótar er ekki ljóst hvaða greinarmun eigi að gera á viðskiptaupplýsingum og fjárhagsupplýsingum skv. grein 9.3. Að lokum varðandi þessi hugtök og kaflann um afritun þá þarf að gæta þess að mögulegt sé að eftirlitsskyldir aðilar geti framfylgt á raunhæfan hátt.

			V. Persónuvernd og fjarskiptalög Vísað er til fyrri umræðu bankans um hvort tilmælin kunni í einhverjum tilvikum að ganga lengra en lög um persónuvernd og fjarskiptalög. Hér er m.a. átt við hvað varðar leiðbeiningar tilmælanna um varðveislu í lengri tíma, en fyrrgreind lög geta í einhverjum tilvikum gert ráð fyrir. Að öðru leyti er vísað til þeirra sjónarmiða og umræðna sem fram komu af hálfu bankans á fundi hans með Fjármálaeftirlitinu þann 21. október sl. og í tölvupóstum, vegna tilmæla þessara og dreifibréfs sem Fjármálaeftirlitið sendi þann 10. október sl.
3.	Arion banki hf.	9.2.3	Sjá almenna umsögn
4.	Arion banki hf.	9.5.1	Sjá almenna umsögn
5.	Lýsing hf.	11.7	Í lið 11.7 í tilmælunum er gerð athugasemd við það að tiltekinn ábyrgðaraðili sé tilnefndur í þjónustusamningi við útvistunaraðila. Nægjanlegt er að fram komi í samningnum að ábyrgðaraðili sé tilnefndur innan fyrirtækisins. Það er ófært að taka þurfi upp þjónustusamninga ef viðkomandi starfsmenn hætta störfum eða þeir breyta um starfssvið hjá eftirslitsskyldum aðilum.
6.	Borgun hf.	12.4	Skýrt er að vottun eftirlitsskylds aðila skv. ISO 27001 staðli jafngildi úttekt skv. lið 12.2, að því gefnu að vottun sé í gildi og umfang vottunar sé í það minnsta hið sama og umfang úttektar sbr. 12.2. Ekki er tiltekið sérstaklega hvort og þá hvaða gögnum vottaðir aðilar þurfa að skila til staðfestingar vottun. Gott væri að fá frekari skýringu á því hvort skila þarf inn staðfestingu á vottun og/eða öðrum gögnum.
7.	Borgun hf.	12.5	Kveðið er á um að Fjármálaeftirliti verði afhentar niðurstöður úttektar óháðs aðila á upplýsingatæknikerfum í gegnum gagnaskilakerfi Fjármálaeftirlits. Borgun getur fallist á það sjónarmið Fjármálaeftirlits að nauðsynlegt sé að fylgst sé með því að bætt verði úr ágöllum innan tilskilinna tímamarka. Borgun telur þó ekki æskilegt að upplýsingar um öryggisveilur séu vistaðar utan kerfa Borgunar. Að mati Borgunar væri hægt að ná fram markmiði greinar 12.5 með því að Fjármálaeftirlit fengi reglulega staðfestingu á því að úrbætur hefðu átt sér stað innan tilskilinna tímamarka. Ekki væri þá þörf á að dreifa sérstaklega upplýsingum um öryggisveilur meðan þær eru enn til staðar.