Réttarreglur um fjármálafyrirtæki sem lúta að upplýsingaöryggi

Málstofa SFF um persónuvernd, 7. júní 2016

Hörður Helgi Helgason

LANDSLÖG

Borgartúni 26
105 Reykjavík
Talsími: 520 2900
Bréfasími: 520 2901
www.landslog.is

Yfirlit

- Gildandi reglur um öryggi persónuupplýsinga
- Öryggiskröfur í sérlögum og stjórnvaldsreglum um fjármálafyrirtæki
  - Skoðun 2014, uppfærð 2016
  - Samanteknar niðurstöður og nokkrar ályktanir sérstaklega um fjármálafyrirtæki
- Næstu skref á vettvangi ESB/EES
  - Ný reglugerð um persónuvernd (*örfá* orð um öryggi)
  - Ný tilskipun um upplýsingaöryggi

Almennar reglur um öryggi persónuupplýsinga

- Lög nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga – meginlögin
  - Gullnu reglurnar, heimildir og réttindi hins skráða
  - En líka reglur um öryggi persónuuppl., 11.-13. gr.
- Reglur nr. 299/2001 um öryggi persónuupplýsinga
  - Byggðar á staðlinum BS7799, nú ISO/IEC 27001:2013
  - Upplýsingaöryggi = Leynd + heilleiki/réttleiki + aðgengi
  - Öryggisstefna, áhættumat og lýsing á öryggisráðstöfunum
  - Að auki: Innra eftirlit og úttektir Persónuverndar

Öryggiskröfur í sérlögum og stjórnvaldsreglum um fjármálafyrirtæki (1 af 6)

- Niðurstöður kynntar í erindi á *Lagadeginum 2014*
- 160 lög skoðuð, 60 lutu að upplýsingaöryggi
- Fimm tegundir réttarreglna voru skoðaðar: Málsmeðferðarreglur; heilbrigðismál; fjármálastarfsemi; fjarskipti og ýmis veitu- og burðarkerfi; lögregla og öryggi ríkisins
- Uppfært 2016: 80 lög um fjármálastarfsemi skimuð, 23 innihéldu ákvæði um upplýsingaöryggi

Öryggiskröfur í sérlögum og stjórnvaldsreglum um fjármálafyrirtæki (2 af 6)

- Helstu ályktanir af skoðuninni:
  - Sjaldan fjallað heildstætt um öryggi
  - Mælt fyrir um sjónarmið en annars vísað í rg.
  - Snúast oft um leynd, en stundum um réttleika eða aðgengileika
  - Sumar lagakröfur tóku í upphafi ekki til upplýsingaöryggis en verður að túlka svo nú

Öryggiskröfur í sérlögum og stjórnvaldsreglum um fjármálafyrirtæki (3 af 6)

Fjármálastarfsemi, 15 helstu lög skoðuð 2016:

- fjármálafyrirtæki, 161/2002
- verðbréfaviðskipti, 108/2007
- kauphallir, 110/2007
- rafræn eignarskráning verðbréfa, 131/1997
- sértryggð skuldabréf, 11/2008
- verðbréfasjóðir, fjárfestingarsjóðir og fagfjárfestasjóðir, 128/2011
- vátryggingastarfsemi, 56/2010
- vátryggingastarfsemi, 56/2010
- vátryggingarsamningar, 30/2004
- miðlun vátrygginga, 32/2005
- opinbert eftirlit með fjármálastarfsemi, 87/1998
- Seðlabanki Íslands, 36/2001
- aðgerðir gegn peningaþvætti og fjármögnun hryðjuverka, 64/2006
- fjarsala á fjármálaþjónustu, 33/2005
- Innheimtulög, 95/2008
- greiðsluþjónusta, 120/2011

Öryggiskröfur í sérlögum og stjórnvaldsreglum um fjármálafyrirtæki (4 af 6)

- Nokkrar ályktanir sérstaklega varðandi lög um fjármálastarfsemi:
  - Algengust eru trúnaðar- og þagnarskylduákvæði, t.d. 58.-60.gr. l. um fjármálafyrirtæki, 5. mgr. 122.gr. l. um verðbréfaviðsk., 13. gr. l. um kauphallir, 113. gr. l. um vátr.samn., 13. gr. l. um miðlun vátr., 13. gr. l. um opinb. eftirl. með fjármálastarfs., 13. gr. innheimtulaga og 2. mgr. 17. og 52. gr. l. um greiðsluþj.
  - Þagnarskylduákvæði vantar hins vegar óvænt annars staðar, t.d. í lög um vátr.starfsemi, í lög um fjarsölu á fjármálaþjónustu og í lög um Viðlagatryggingu Íslands.

Öryggiskröfur í sérlögum og stjórnvaldsreglum um fjármálafyrirtæki (5 af 6)

- Nokkrar ályktanir sérstaklega varðandi lög um fjármálastarfsemi:
  - Afar fá lög innihalda almennar skyldur um upplýs.öryggi, sbr. þó t.d. 19. gr. b í lögum um fjármálafyrirtæki og 13. gr. l. um rafræna eignaskráningu verðbréfa.
  - Mörg laganna innihalda kröfur um innra eftirlit og áhættustýringu, t.d. 1. mgr. 20. gr. l. um útg. og meðferð rafeyris og 1. mgr. 15. gr. l. um greiðsluþjónustu, en taka oftast ekki eða óljóst til upplýsingaöryggis, t.d. 2. mgr. 6. gr. l. um verðbr.viðsk. og ákvæði laga um vátr.starfsemi, svo sem 5. tl. 1. mgr. 20. gr., 40. gr. og 4. mgr. 63. gr.

Öryggiskröfur í sérlögum og stjórnvaldsreglum um fjármálafyrirtæki (6 af 6)

- Nokkrar ályktanir sérstaklega varðandi lög um fjármálastarfsemi:
  - Engin laganna mæla fyrir um tilteknar öryggisráðstafanir.
  - Oftast kveðið á um skyldu til að veita aðgang, oftast til FME, úrskurðarnefnda eða annarra opinberra aðila, t.d. 3. mgr. 25. gr. l. um rafræna eignaskráningu verðbréfa, VI. k. og 31. gr. laga um kauphallir, auk 1. mgr. 19. gr. b, 29. gr. c og 2. og 3. mgr. 107. gr. l. um fjármálafyrirtæki.
  - Einstaka sinnum vísað til persónuverndarlaga eða Persónuverndar, t.d. 73. gr. l. um greiðsluþjónustu og 2. mgr. 14. gr. laga um rafr. eignaskráningu verðbréfa

Næstu skref á vettvangi ESB/EES (1 af 3)

- Ný reglugerð ESB um persónuvernd = viðfangsefni næsta fyrirlestrar, en rétt örfá orð hér um nýjan kafla í henni um upplýsingaöryggi:
  - Verja skal uppl. með viðeig. öryggisráðstöfunum
  - Sýna má hlítingu við öryggiskröfur með því að nýta verklagsreglur starfsgreinar (Code of Conduct)
  - Tilkynna skal öryggisbrot til PV innan 72 klst. og í sumum tilvikum beint til hins skráða

Næstu skref á vettvangi ESB/EES (2 af 3)

- Ný tilskipun um upplýsingaöryggi
  - „Directive concerning measures to ensure a high common level of network and information security across the Union“, COM(2013) 48 final / 2013/0027 (COD)
  - Búist við afgreiðslu Evrópuþings í júlí og birtingu í ágúst
  - Tekur til „public administrators“, en einnig „market operators“, sem eru „operators of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of […] banking, stock exchanges […]“ og „central counterparty clearing houses“

Næstu skref á vettvangi ESB/EES (3 af 3)

- Ný tilskipun um upplýsingaöryggi
  - Fellir fjármálafyrirtæki afdráttarlaust undir þá sem reka „ómissandi upplýsingainnviði“, sbr. 27. tl. 3. gr. fjarskiptal.
  - Setur skýrari reglur um CERT-hópa, sbr. netöryggissveit PFS (I.k.) og samstarf CERT-hópa (II.k.), en tiltekur einnig lágmarkskröfur varðandi upplýsingaöryggi sem uppfylla skal af rekstraraðilum ómissandi upplýsingainnviða (III.k.) að viðlögðum viðurlögum (IV.k.)
  - Frestur til innleiðingar er eitt og hálft ár, þ.e. til ársloka 2017.

Spurningar?

hhh@landslog.is
www.landslog.is
@HHelgi