
BBA // FJELDCO

Hádegisfundur Ský

Ábyrgð stjórnenda í kjölfar netárásar

Thelma Christel Kristjánsdóttir, LL.M., lögmaður

BBA // FJELDCO

facebook

- Alríkisviðskiptanefndin
  (e. Federal Trade Commission, FTC)
  sektaði META/Facebook um fimm milljarða dollara.

"Facebook's violations were a direct result of the company's behavioural advertising business model.

"The proposed settlement does little to change the business model or practices that led to the recidivism."

Rohit Chopra, nefndarmeðliðmur Alríkisviðskiptanefndar (FTC) 2018-2021

"The proposed settlement lets Facebook off the hook for unspecified violations."

"The grant of immunity for Facebook's officers and directors is a giveaway."

Rohit Chopra, nefndarmeðlimur
Alríkisviðskiptanefndar (FTC) 2018-2021


DRIZLY

Hvað gerðist?

Þjálfun starfsfólks ábótavant og öryggiskerfi uppfylltu ekki kröfur

Lykilorð inn á AWS kerfið ekki nógu örugg og ekki lokað nægjanlega hratt á aðgang verktaka

Engar veikleika-prófanir og ekki leitað eftir ólögmætum flutningi gagna um viðskipta-vini út fyrir sín kerfi

Hver voru viðurlögin?

- Setja upp fullnægjandi öryggiskerfi sem metið yrði af utanaðkomandi aðilum
- Eyða óþarfa gögnum
- Takmarka gagnasöfnun til framtíðar
- Persónuleg ábyrgð stjórnanda
- Gildir í 20 ár

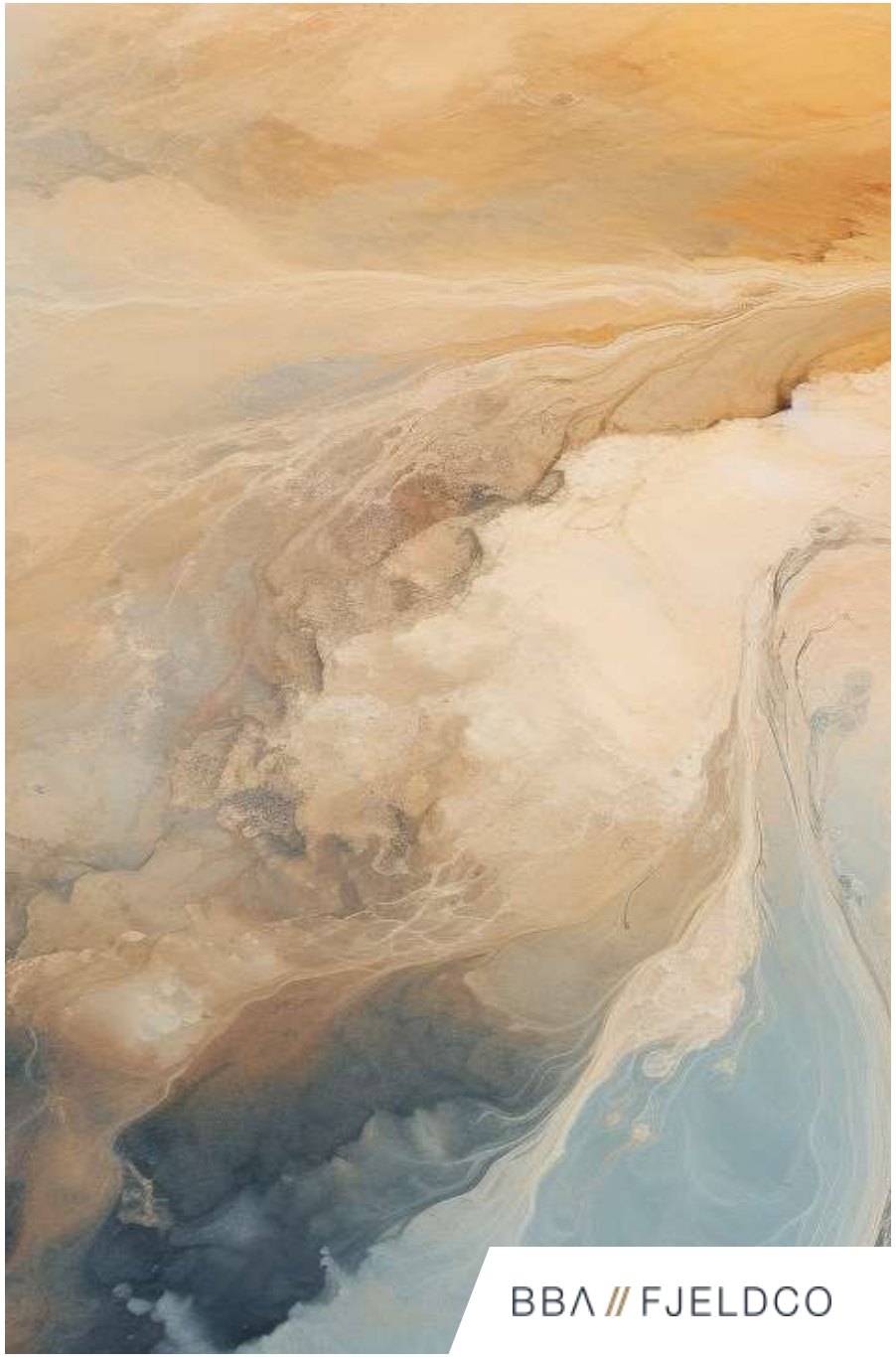
THE HOME DEPOT

- Bloggsíða birtir upplýsingar um öryggisbrest hjá byggingavöruversluninni Home Depot
- Við skoðun kemur í ljós að 56 milljónum kortanúmera hafði verið lekið
- Bresturinn tilkynntur án tafar til fjármálaeftirlitsins (e. Securities and Exchange Commission, SEC). Rannsókn hefst strax og fjárfestar upplýstir

Eftirköst

- Hluthafar fara í mál vegna trúnaðarbrests
  - Náðu ekki að sýna fram á að það hefði verið athafnaskylda
  - “Business Judgement Rule”

Hvað með Evrópu og Ísland?



Ísland

- Bótaábyrgð stjórnenda sambærileg við BJR (Home Depot)
- NISD: innleitt með lögum nr. 78/2019 -> NISD2 á leiðinni og aðildarríki ESB höfðu innleiðingarfrest til 17. október nk.
- DORA -> Tekur gildi í Evrópu í janúar 2025

Bótagrundvöllur viðskiptaákvarðana (BJR eins og í Home Depot)

- „Business Judgment Rule“ / „Internal Management Rule“.

- Þessi regla virðist birtast skýrt í héraðsdómi, sem Hæstiréttur staðfesti með vísan til forsendna, sbr. dóma Hæstaréttar frá 14. janúar 2010 í máli nr. 350/2009 (Straumur-Burðarás hf.) og 2. október 2003 í máli nr. 40/2003 (Otislyftur).

HÆSTIRÉTTUR ÍSLANDS

„Stjórnendur félags taka ákvarðanir um fjárhagslegar ráðstafanir og geta dómstólar ekki fjallað um hvort þær hafi verið nauðsynlegar eða ekki. Auk þess er tekið fram að stefnendum hafi með öllu mistekist að sanna tjón sitt.“ - Nr. 350/2009 - 14. janúar 2010 (Straumur-Burðarás)

HÆSTIRÉTTUR ÍSLANDS

„Í þessu samhengi er rétt að huga að því að þegar viðskiptaákvarðanir stjórnenda fyrirtækja eru metnar verður að líta til þess að um er að ræða ákvarðanir sem oftar en ekki fela í sér vissa áhættu og ekki er alltaf einsýnt um hvort forsendur allar standist þegar upp er staðið. Er það því mat dómsins að stefnandi hafi ekki í ákvörðunum sínum fyrir félagið tekið meiri áhættu en honum var heimilt að taka miðað við þær forsendur sem virðast hafa legið fyrir.“ - Nr. 350/2009 - 14. janúar 2010 (Otis Lyftur)

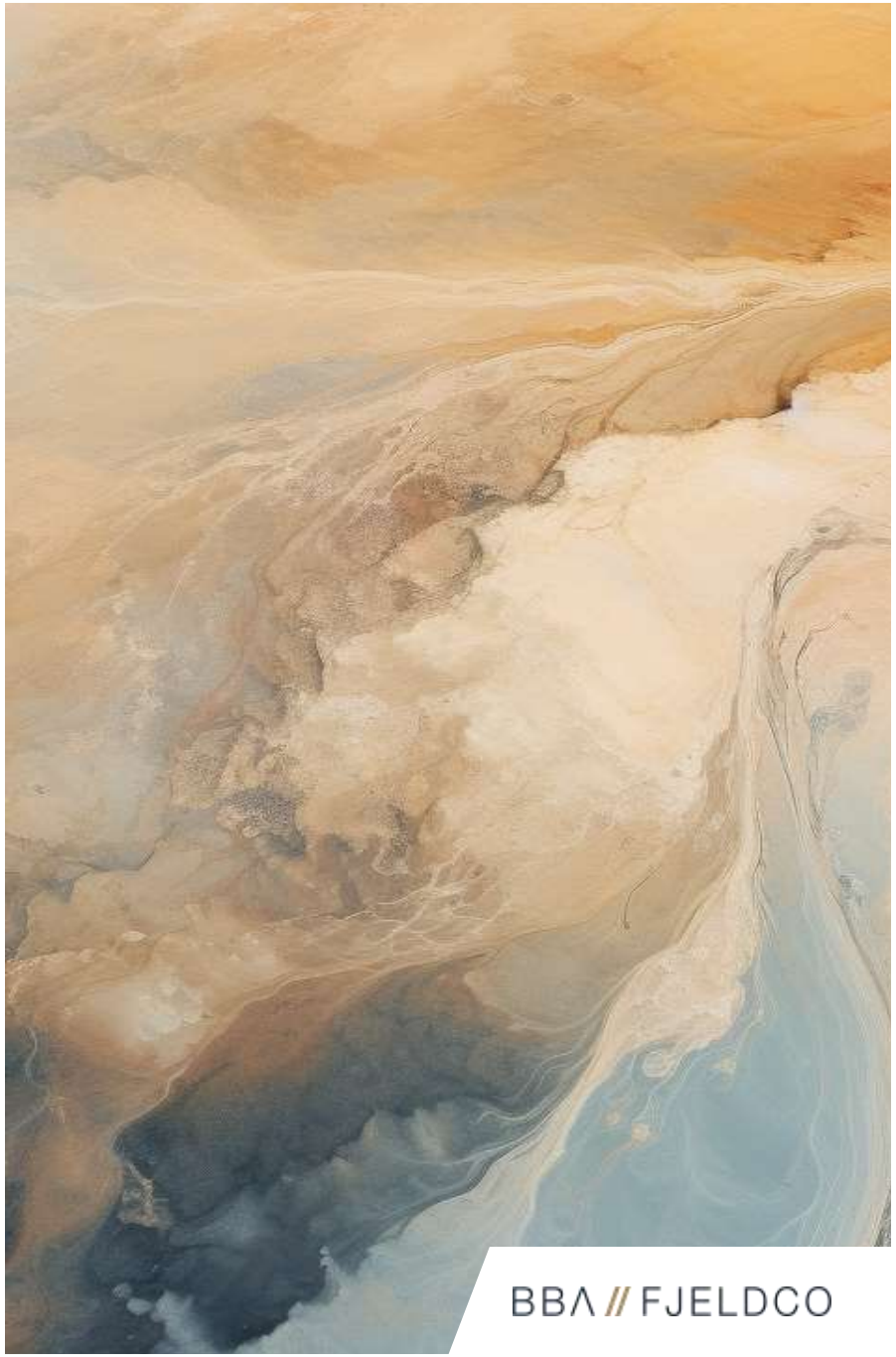
Bótaábyrgð íslenskra stjórnenda

- Stjórnarmenn verða almennt ekki gerðir ábyrgir fyrir því að taka rangar ákvarðanir í málefnum félaga heldur þarf meira að koma til.
- Ef mat þeirra er augljóslega rangt, ef þeir vanrækja að kynna sér mikilvæg málefni eða ef þeir brjóta þær skyldur sem lög eða samþykktir leggja þeim á herðar getur orðið um bótaskyldu að ræða, t.d. ef þeir láta stjórnast af persónulegum hagsmunum eða ef um einhvers konar óreiðu er að ræða í starfsemi þess félags sem þeir stjórna.

Bótagrundvöllur

- Athafnaleysi.
- Stjórnarmenn hafa vissar lágmarksskyldur til þess að hafa eftirlit með starfsemi félagsins og til þess að gæta þess að farið sé að lögum og samþykktum þess. Almennt má fullyrða að stjórnarmönnum félags beri að kynna sér rekstur félagsins í aðalatriðum og mikilsháttar ráðstafanir

NISD 2



NIS 2 Scope expansion

✚ New sub-sectors added by NIS 2

New sector

NIS 1

7 Operators of Essential Services **(OES)**:

- Energy
- Transport
- Banking
- Drinking Water
- Health sector
- Financial market infrastructures
- Digital Infrastructure

3 Digital Services Providers **(DSP)**:

- Search engine
- E-commerce websites
- Cloud services

NIS1 total: 30 types of entities

NIS 2

11 sectors identified as **Sector of High Criticality** *(Annex 1)*

- Energy ✚
- Transport ✚
- Banking ✚
- Financial market infrastructures
- Health ✚
- Drinking Water
- Waste water
- Digital Infrastructure ✚
- ICT services management (B2B)
- Public administration
- Space

New: 7 sectors identified as **Critical Sectors** *(Annex 2)*

- Postal & courier services
- Waste management
- Chemicals
- Food
- Manufacturing
- Digital providers
- Research

New: Inclusion of the **supply chain**

New: Inclusion of **SMEs under certain criteria**

NIS2 total: 67 types of entities

Point of attention > NIS 2 leaves Member States to extend this list during transposition if they so choose, as they have done previously with NIS 1 (ex. National extensions of NIS to education, social service).

Kröfur á fyrirtæki

Lágmarkskröfur um áhættu-stýringu og viðbúnað

Tilkynningar-skylda til netöryggis-sveitar, þ. á m. um útvistunarfyrir-komulag

Tilkynningarskylda til almennings ef almennings-vitundar er þörf eða af öðrum ástæðum nauðsynlegt vegna almannahagsmuna

Viðurlög

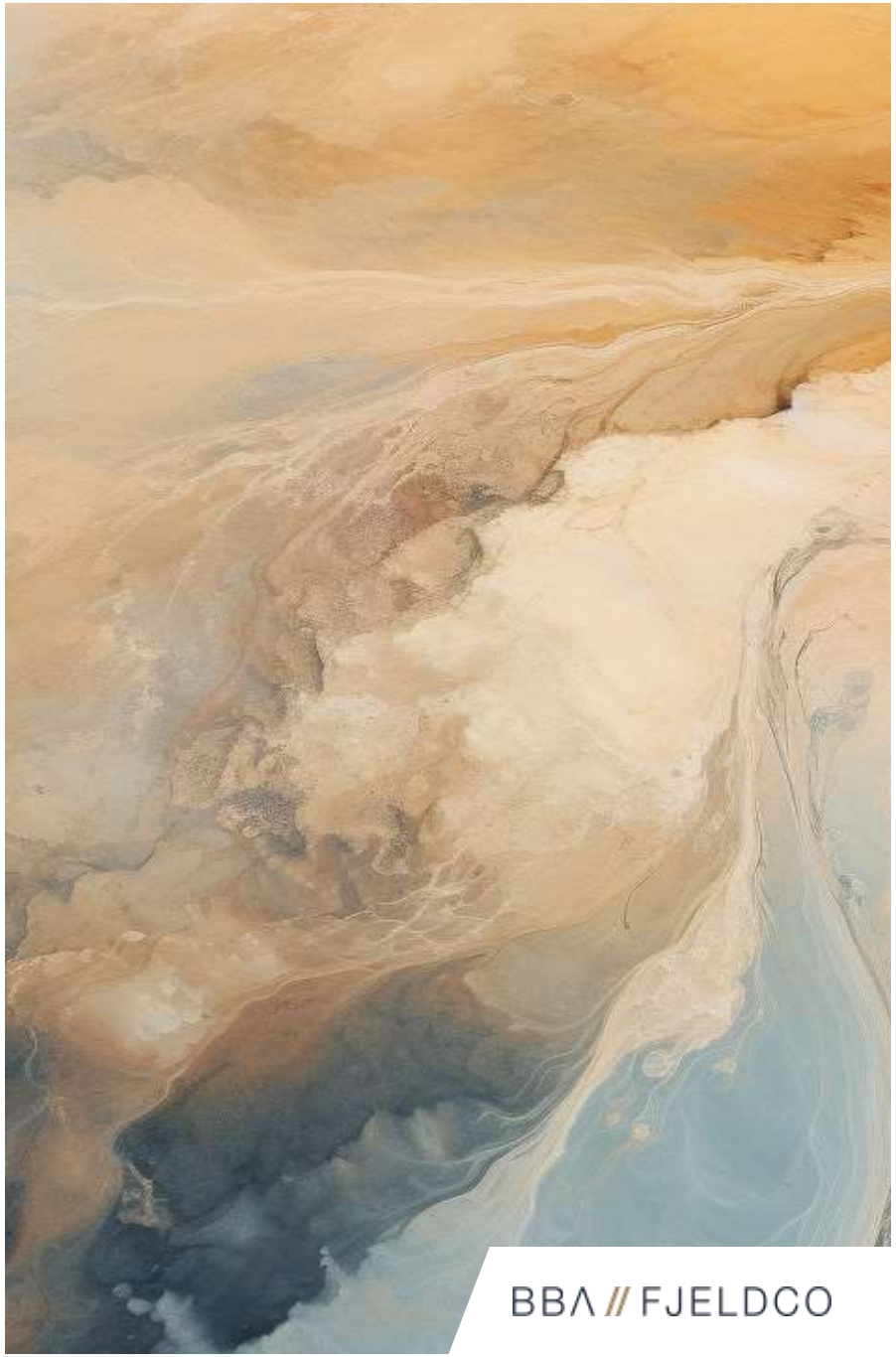
- Dagsektir allt að 500.000 kr. á dag
- Stjórnvaldssektir sem fara hækkandi
- Allt að tveggja ára fangelsi
- Bótaábyrgð

Breytingar með NISD2 – ábyrgð stjórnenda

Yfirstjórn fyrirtækis ber ábyrgð á að skyldur um fullnægjandi öryggi séu uppfylltar

Sérstaklega tekið fram að stjórn fyrirtækis beri ábyrgð á að innleiða fullnægjandi verklag netöryggis

DORA



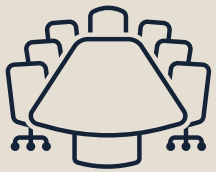
DORA í stuttu máli

- Tekur gildi í janúar 2025
- Setur reglur um netöryggi í fjármálageiranum með tilteknum reglum um;
  - Netöryggisstefnu og áhættustjórnun
  - Tilkynningarskyldu um netöryggisatvik
  - Áreiðanleikaprófanir
  - Meginreglur til að hafa áhrif á áhættu vegna þriðju aðila
  - Skylda til að deila upplýsingum um netöryggisógnir

Kröfur á æðstu stjórnendur (e. management body)

Bera endanlega ábyrgð á netöryggi

Þurfa að hafa fullnægjandi þekkingu á netöryggi



„Managament body“ væri í flestum tilvikum stjórnarmenn

Setja, yfirfara og endurskoða reglulega lykilstefnur, áætlanir og almennt netöryggi

Halda netöryggis-þekkingu sinni við og fá reglulegar skýrslur frá kerfisstjórum.

BBA // FJELDCO

Samantekt

- Hingað til hafa eingöngu verið lágmarksskyldur á stjórnarmenn til athafna
- Athafnir stjórnarmanna einnig metnar á þeim grundvelli að dómstólar meti ekki fjárhagsákvarðanir eftir á sem og að litið sé til þess að flestum ákvörðunum fylgi einhver áhætta
- Nú munu DORA og NIS2 hins vegar bæði skýra skyldur þeirra stjórnarmanna sem falla undir gildissvið þeirra og setja endanlega ábyrgð á netöryggi á þá.
- Auk þess kveður NIS2 skýrlega á um persónulega ábyrgð stjórnarmanna


Takk fyrir!
BBA // FJELDCO