

## REGLUGERÐ

### um breytingu á reglugerð um öryggi net- og upplýsingakerfa veitenda stafrænnar þjónustu, nr. 1255/2020.

#### 1. gr.

Í stað heitisins „Póst- og fjarskiptastofnun“ í 4. tölulið 1. mgr. 3. gr. reglugerðarinnar og sama orðs hvarvetna annars staðar í reglugerðinni, komi í viðeigandi beygingarfalli: Fjarskiptastofa.

#### 2. gr.

Fyrirsögn III. kafla reglugerðarinnar verður: **Tæknilegar og skipulagslegar ráðstafanir.**

#### 3. gr.

Eftirtaldar breytingar verða á 7. gr. reglugerðarinnar:

- a. 3. málslíður 1. mgr. fellur brott.
- b. Orðin „sem og raunlæga vernd öryggisrýma, sbr. 12. gr.“ í 1. málslíð 2. mgr. falla brott.
- c. Við ákvæðið bætist ný málsgrein, sem orðast svo:

Með hliðsjón af alþjóðlegum viðmiðum um bestu framkvæmd skulu öryggisráðstafanir tryggja öryggisstig net- og upplýsingkerfa sem hæfir áhættunni sem stafar af og skulu þær a.m.k. fela í sér:

  - a. öryggi kerfa og aðstöðu;
  - b. meðhöndlun atvika;
  - c. stjórnun rekstrarsamfellu;
  - d. eftirlit, úttektir og prófanir;
  - e. hlítu við alþjóðlega viðurkennda staðla um bestu framkvæmd.

#### 4. gr.

Í stað 8. og 9. gr. reglugerðarinnar koma fimm nýjar greinar, ásamt fyrirsögnum, sem verða 8., 9., 10., 11. og 12. gr. og orðast þær svo:

##### a. (8. gr.)

#### *Öryggi kerfa og aðstöðu.*

Þær ráðstafanir sem varða öryggi kerfa og aðstöðu skv. a-lið 4. mgr. 7. gr., en með því er átt við öryggi net- og upplýsingakerfa og efnislegs umhverfis þess, skulu fela í sér:

- a. kerfisbundna stýringu á net- og upplýsingakerfum sem felur í sér að kortleggja upplýsingakerfi og ákvarða viðeigandi stefnu um stjórnun upplýsingaöryggis, þ.m.t. áhættugreiningu, mannaud, rekstraröryggi, öryggishönnun, örugga vistferilsstjórnun gagna og kerfa sem og, eftir atvikum, dulkóðun og stýringu þess;
- b. raunlægt og umhverfislegt öryggi sem felur í sér tiltækar ráðstafanir til að vernda öryggi net- og upplýsingakerfa, sem veitendur stafrænna þjónustu nota, gegn skemmdum með því að nota áhættumiðaða nálgun sem tekur til hvers konar áhættu, t.d. vegna kerfisbilunar, mannlegra mistaka, skaðlegra aðgerða eða náttúrufyrirbæra;
- c. aðfangaöryggi, sem felur í sér að ákvarða þurfi og viðhalda viðeigandi stefnu til að tryggja tiltækileika mikilvægra aðfanga sem eru notuð í tengslum við veitingu þessarar þjónustu og, eftir atvikum, að tryggja rekjanleika þessara aðfanga;
- d. eftirlit með aðgangi að net- og upplýsingakerfum sem felur í sér tiltækar ráðstafanir til að tryggja að raunlægur og kerfislegur aðgangur að net- og upplýsingakerfum, þ.m.t. stjórnsýslu-öryggi net- og upplýsingakerfa, sé heimilaður og takmarkaður á grunni viðskipta- og öryggis-krafna.

##### b. (9. gr.)

#### *Meðhöndlun atvika.*

Þær ráðstafanir sem varða meðhöndlun atvika skv. b-lið 4. mgr. 7. gr. skulu fela í sér:

- a. viðhald og prófun á ferlum og verklagsreglum fyrir greiningu til að tryggja að fullnægjandi vitneskja fáiist um óeðlilega atburði með tímanlegum hætti;
- b. ferli og stefnu varðandi tilkynningu atvika og auðkenningu galla og veikleika í upplýsingakerfi þeirra;
- c. viðbrögð við atvikum í samræmi við settar verklagsreglur og skýrslugjöf um árangur ráðstafana sem gripið var til;
- d. mat á alvarleika atviksins, greinargerð um þá vitneskju sem fengist hefur við greiningu atviksins og söfnun viðeigandi upplýsinga, sem kunna að færa sönnur á atvikið og stuðla að samfelldu ferli úrbóta.

c. (10. gr.)

*Stjórnun rekstrarsamfellu.*

Þær ráðstafanir sem varða stjórnun rekstrarsamfellu skv. c-lið 4. mgr. 7. gr., en með því er átt við getu fyrirtækisins til að viðhalda eða, eftir atvikum, hefja á ný veitingu þjónustu á viðunandi og fyrir fram skilgreindum stigum í kjölfar atviks sem hefur skerðandi áhrif. Ráðstafanirnar skulu fela í sér:

- a. undirbúning og notkun viðbragðsáætlana á grunni rekstraráhrifagreiningar til að tryggja samfellu í þeirri þjónustu sem veitendur stafrænnar þjónustu veita; meta skal og prófa áætlanirnar með reglulegu millibili, t.d. með æfingum;
- b. endurreisnargetu vegna stóráfalla sem skal metin og prófuð með reglulegu millibili, t.d. með æfingum.

d. (11. gr.)

*Innra eftirlit.*

Þær ráðstafanir sem varða eftirlit, úttektir og prófanir skv. d-lið 4. mgr. 7. gr. skulu fela í sér setningu stefna, sem uppfæra skal reglulega, um:

- a. framkvæmd skipulagðrar runu athugana eða mælinga til að meta hvort net- og upplýsingakerfi virki eins og ætlast er til;
- b. skoðun og sannprófun til að hafa eftirlit með því hvort stöðluðum viðmiðunarreglum eða safni viðmiðunarreglna sé fylgt, skráningar séu nákvæmar og hvort markmiðin um skilvirkni og árangur séu uppfyllt;
- c. ferli sem ætlað er að leiða í ljós galla í öryggisbúnaði net- og upplýsingakerfis sem verndar gögn og viðheldur þeirri virkni sem ætlast er til. Slíkt ferli skal fela í sér tæknilegt vinnsluferli og starfsfólk sem tekur þátt í rekstrinum.

e. (12. gr.)

*Sannprófun við hlítu krafna.*

Veitendur stafrænnar þjónustu skulu tryggja að þeir hafi undir höndum fullnægjandi gögn til að gera Fjarskiptastofu kleift að sannprófa hlítu við þær kröfur sem fram koma í þessum kafla.

5. gr.

Eftirfarandi breytingar verða á 10. gr. reglugerðarinnar:

- a. 2. og 3. málslíður 2. mgr. fellur brott.
- b. 10. gr. reglugerðarinnar verður 13. gr. sem verður hluti af III. kafla

6. gr.

Greinar 11 til og með 17 í reglugerðinni falla brott og þar með IV. kafli, Tæknilegar ráðstafanir, og breytast aðrir kaflar og aðrar greinar sem eftir koma til samræmis við það.

7. gr.

Heitið „Póst- og fjarskiptastofnunar“ í 1. mgr. 18. gr. reglugerðarinnar fellur brott.

8. gr.

Reglugerð þessi er sett með heimild í 7., 8. og 28. gr. laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða, og öðlast þegar gildi.

*Innviðaráðuneytinu, 4. júní 2025.*

**Eyjólfur Ármannsson.**

---

*Aðalsteinn Þorsteinsson.*

---

B-deild – Útgáfudagur: 12. júní 2025