Lagalega hliðin á skýinu

Erum við berskjölduð í skýinu? Hádegisfundur faghóps Ský um öryggismál

Grand Hótel, 23. október 2019

Hörður Helgi Helgason

LANDSLÖG

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

Tveir mikilvægir sjónarhólar, þó ekki þeir einu

1. **Persónuvernd**: Hér á landi eru í gildi sérstakar réttarreglur um vinnslu upplýsinga sem verða raktar til tiltekinna einstaklinga, svonefndar „persónuupplýsingar“, þ.e. lög nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga (hér, pvl.) sem innleiddu almennu pv-reglugerð ESB 2017/679 (hér, pvrg.). Meðal ákvæða pvl. og pvrg. eru ákvæði um að gæta skuli að öryggi þessara upplýsinga.
2. **Öryggi mikilvægra innviða**: Ný lög sem taka gildi næsta haust gera kröfur til öryggis net- og upplýsingakerfa svonefndra „mikilvægra innviða“, þ.e. lög nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða (hér, öil.) sem innleiddu svonefnda netöryggistilskipun ESB 2016/1148 (hér, öitsk.).

1. Persónuvernd – Meginreglur um öryggi

- **Meginreglur um vinnslu (gullnu reglurnar)**: Í 8. gr. pvl. eru settar fram meginreglur um alla vinnslu persónuupplýsinga:
  - 2. tl.: Frekari vinnsla í sagnfræðilegum, tölfræðilegum eða vísindalegum tilgangi ekki ósamrýmanleg ef „viðeigandi öryggis“ gætt.
  - 4. tl.: Gæta skal að því að persónuupplýsinga séu „áreiðanlegar og uppfærðar eftir þörfum“.
  - 5. tl.: Geyma má persónuupplýsingar lengur en nauðsynlegt vegna tilgangs ef í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi og „viðeigandi öryggis sé gætt“.
  - 6. tl. Gæta skal að því að persónuupplýsingar „séu unnar með þeim hætti að viðeigandi öryggi persónuupplýsinganna sé tryggt“.

1. Persónuvernd – Almenn ákvæði um öryggi

- **Öryggi persónuupplýsinga**: Skv. 27. gr. pvl. skulu ábyrgðar-/vinnsluaðilar:

  „gera viðeigandi tæknilegar og skipulagslegar ráðstafanir til að tryggja viðunandi öryggi persónuupplýsinga með hliðsjón af nýjustu tækni, kostnaði við framkvæmd, eðli, umfangi, samhengi og tilgangi vinnslunnar og áhættu, mislíklegri og misalvarlegri, fyrir réttindi og frelsi einstaklinga“

  Í 2. mgr. 32. gr. pvrg. er mælt fyrir um áhættumat og í 1. mgr. um að velja skuli öryggisráðstafanir.

  Skv. 3. gr. reglna nr. 299/2001 um öryggi persónuupplýsinga skal útbúa öryggiskerfi í þremur áföngum: Öryggisstefna – áhættumat – lýsing á öryggisráðstöfunum.

- **Tilkynningar um öryggisbresti**: 27. gr. pvl. Afar skammur frestur (72 klst.).

1. Persónuvernd – Skyld ákvæði um öryggi

- **Mat á áhrifum á persónuvernd (MÁP)**: Skv. 29. gr. pvl. skal leggja „mat á áhrifum fyrirhugaðra vinnsluaðgerða á vernd persónuupplýsinga“ ef líklegt að í vinnslu felist mikil áhætta „fyrir réttindi og frelsi einstaklinga“. Persónuvernd *„leggur mikla áherslu á að persónuupplýsingar séu ekki vistaðar í tölvuskýjum nema að undangengnu ítarlegu áhættumati“*.

  Fjr., í leiðbein. 2016 til ríkisstofnana um notkun á tölvuskýjum: Innleiðing í fjórum skrefum (Þarfagreining – Áhættumat – Kröfulýsing – Samningagerð) og gátlisti (*ekki* tæmandi heldur „atriði sem huga ber að“).

- **Innbyggð og sjálfgefin persónuvernd**: Í 1. mgr. 25. gr. pvrg., sbr. 24. gr. pvl.:

  „[…] skal ábyrgðaraðili […] gera […] ráðstafanir […] sem hannaðar eru til að framfylgja meginreglum um persónuvernd […] og fella nauðsynlegar verndarráðstafanir inn í vinnsluna til að uppfylla kröfur [pvrg.] og vernda réttindi [hinna skráðu]“

1. Persónuvernd – Önnur ákvæði

- **Flutningur út fyrir EES**: Skv. 44. gr. pvrg. er einungis heimilt að miðla persónuupplýsingum út fyrir EES ef til staðar er sérstök heimild, þ.e.:
  - ákvörðun framkvæmdastjórnar ESB um að beitt sé fullnægjandi vernd, sbr. 45. gr. og augl. 228/2017 og ákv. ESB 2016/1250 um friðhelgisskjöld (e. Privacy Shield);
  - „viðeigandi verndarráðstafanir“, svo sem bindandi fyrirtækjareglur, stöðluð samningsákvæði eða leyfi Persónuverndar, sbr. 46. og 47. gr.; eða
  - „undanþágur vegna sérstakra aðstæðna“, svo sem upplýst samþykki sérhvers skráðs eða nauðsyn vegna samningsalmannahagsmunir, sbr. 49. gr.

  48. gr. pvl.: Ekki viðurkenna erl. dóma nema skv. samn. og beiðni: Cloud Act.
- **Vinnsluaðilar og -samningar**: Fyrirmæli ábyrgðaraðila, undirvinnsluaðilar, rekstraröryggi vs. vörslur/yfirráð, eyða/skila uppl. og „öllum afritum“: 28. gr.

2. Öryggi innviða – Skilgreiningar og gildissvið

- **Hvað er „skýjavinnsluþjónusta“**: Í öil. og öitsk. er hugtakið „skýjavinnsluþjónusta“ (e. „cloud computing service“) skilgreint sem *„Stafræn þjónusta sem veitir aðgang að skalanlegum og sveigjanlegum brunni tölvunargetu sem hægt er að deila.“* Hins vegar er „skýjavinnsluþjónusta“ einungis notað í gildissviðsákvæði laganna og skilgreiningu á „stafrænni þjónustu“ (hringskilgreining).
- **Gilda um kerfi „rekstraraðila nauðsynlegrar þjónustu“**: Til þeirra teljast:

  „[N]et- og upplýsingakerfi rekstraraðila nauðsynlegrar þjónustu hér á landi á sviði bankastarfsemi og innviða fjármálamarkaða, flutninga, heilbrigðisþjónustu, orku-, hita- og vatnsveitna, svo og stafrænna grunnvirkja, að uppfylltum skilyrðum 3. gr.

  Lög þessi gilda jafnframt um net- og upplýsingakerfi veitenda stafrænnar þjónustu sem starfrækja netmarkað, leitarvél á netinu eða skýjavinnsluþjónustu, þó ekki veitendur stafrænnar þjónustu sem teljast örfélög í skilningi laga um ársreikninga.“

2. Öryggi innviða – Ákvæði

- **Áhættustýring og viðbúnaður**: Samkvæmt 7. gr. öil. skulu mikilvægir innviðir skjalfesta stefnu og ferla til að „meta, stýra og lágmarka“ hættur gegn net- og upplýsingakerfum þeirra.
- **Tilkynning til netöryggissveitar**: Skv. 8. sbr. 15. gr. skulu mikilvægir innviðir tilkynna netöryggissveit um „alvarleg atvik eða áhættu sem ógnar öryggi“ og gera skal öðrum kleift að miðla til sveitarinnar tilkynningum.

hhh@landslog.is
@HHelgi
landslog.is