

Lög

um breyting á lögum um persónuvernd og meðferð persónuupplýsinga, nr. 77 23. maí 2000.

1. gr.

6. gr. laganna orðast svo:

Lögin gilda um vinnslu persónuupplýsinga á vegum ábyrgðaraðila sem hefur staðfestu hér á landi, enda fari vinnsla persónuupplýsinganna fram á Evrópska efnahagssvæðinu eða í landi eða á stöðum sem Persónuvernd auglýsir í Stjórnartíðindum.

Lögin gilda einnig um vinnslu persónuupplýsinga þótt ábyrgðaraðili hafi staðfestu í ríki utan Evrópska efnahagssvæðisins ef hann notar tæki og búnað sem er hér á landi.

Lögin gilda einnig um vinnslu upplýsinga um fjárhagsmálefni og lánstraust lögaðila, sbr. 45. gr. laganna, enda þótt ábyrgðaraðili hafi ekki staðfestu hér á landi, ef hann notar tæki og búnað sem er hér á landi.

Ákvæði 2. og 3. mgr. gilda ekki ef umræddur tækjabúnaður er einungis notaður til að flytja persónuupplýsingar um Ísland.

Þegar svo hagar til sem greinir í 2. og 3. mgr. skal ábyrgðaraðili tilnefna fulltrúa sinn sem hefur staðfestu hér á landi og gilda þá ákvæði laganna varðandi ábyrgðaraðila um þann fulltrúa eftir því sem við á.

2. gr.

Eftirfarandi breytingar verða á 7. gr. laganna:

- Við bætist ný málsgrein, svohljóðandi:
Ábyrgðaraðili ber ábyrgð á því að vinnsla persónuupplýsinga uppfylli ávallt ákvæði 1. mgr.
- Fyrirsögn greinarinnar orðast svo: *Meginreglur um gæði gagna og vinnslu.*

3. gr.

Eftirfarandi breytingar verða á 8. gr. laganna:

1. tölul. 1. mgr. orðast svo: hinn skráði hafi ótvírætt samþykkt vinnsluna eða veitt samþykki skv. 7. tölul. 2. gr.
- Við greinina bætist ný málsgrein svohljóðandi:
Persónuvernd getur heimilað vinnslu persónuupplýsinga í öðrum tilvikum en greinir í 1. og 2. mgr. ef sýnt þykir að brýnir almannahagsmunir eða hagsmunir einstaklinga,

þar með taldir hagsmunir hins skráða, krefjist þess. Skal þá ótvírætt að þörfin fyrir vinnsluna vegi þyngra en tillitið til þess að hún fari ekki fram. Getur Persónuvernd bundið slík leyfi þeim skilyrðum sem hún metur nauðsynleg hverju sinni til að tryggja hagsmuni hins skráða.

- c. Fyrirsögn greinarinnar orðast svo: *Almennar reglur um heimildir fyrir vinnslu persónuupplýsinga.*

4. gr.

Eftirfarandi breytingar verða á 9. gr. laganna:

- a. Í stað orðanna „Vinnsla viðkvæmra persónuupplýsinga er óheimil nema einhver af eftirfarandi þáttum eigi við“ í 1. mgr. kemur: Vinnsla viðkvæmra persónuupplýsinga er óheimil nema uppfyllt sé eitthvert af skilyrðum 1. mgr. 8. gr. og enn fremur eitthvert af eftirfarandi skilyrðum.
- b. Fyrirsögn greinarinnar orðast svo: *Sérstök skilyrði fyrir vinnslu viðkvæmra persónuupplýsinga.*

5. gr.

11. gr. laganna orðast svo ásamt fyrirsögn:

Áhættumat, öryggi og gæði persónuupplýsinga.

Ábyrgðaraðili skal gera viðeigandi tæknilegar og skipulagslegar öryggisráðstafanir til að vernda persónuupplýsingar gegn ólöglegri eyðileggingu, gegn því að þær glatist eða breytist fyrir slysi og gegn óleyfilegum aðgangi.

Beita skal ráðstöfunum sem tryggja nægilegt öryggi miðað við áhættu af vinnslunni og eðli þeirra gagna sem verja á, með hliðsjón af nýjustu tækni og kostnaði við framkvæmd þeirra.

Ábyrgðaraðili ber ábyrgð á því að áhættumat og öryggisráðstafanir við vinnslu persónuupplýsinga séu í samræmi við lög, reglur og fyrirmæli Persónuverndar um hvernig tryggja skuli öryggi upplýsinga, þ.m.t. þá staðla sem hún ákveður að skuli fylgt.

Ábyrgðaraðili ber ábyrgð á því að áhættumat sé endurskoðað reglulega og öryggisráðstafanir endurbættar að því marki sem þörf krefur til að uppfylla ákvæði þessarar greinar.

Ábyrgðaraðili skal skrá með hvaða hætti hann mótar öryggisstefnu, gerir áhættumat og ákveður öryggisráðstafanir. Skal Persónuvernd hafa aðgang að upplýsingum um framangreind atriði hvenær sem hún óskar.

6. gr.

12. gr. laganna orðast svo:

Ábyrgðaraðili skal viðhafa innra eftirlit með vinnslu persónuupplýsinga til að ganga úr skugga um að unnið sé í samræmi við gildandi lög og reglur og þær öryggisráðstafanir sem ákveðnar hafa verið.

Innra eftirlit skal viðhaft með reglubundnum hætti. Tíðni eftirlitsins og umfang þess skal ákveðið með hliðsjón af áhættunni sem er samfara vinnslunni, eðli þeirra gagna sem unnið er með, þeirri tækni sem notuð er til að tryggja öryggi upplýsinganna og kostnaði af framkvæmd eftirlitsins. Það skal þó eigi fara fram sjaldnar en árlega.

Ábyrgðaraðili skal sjá til þess að gerð sé skýrsla um hverja aðgerð sem er liður í innra eftirliti. Í slíkri skýrslu skal lýsa niðurstöðu hvers þáttar eftirlitsins. Skýrslur um innra eftirlit skal varðveita tryggilega. Persónuvernd hefur rétt til að aðgangs að þeim hvenær sem er.

Persónuvernd getur sett frekari fyrirmæli um framkvæmd innra eftirlits og veitt undanþágu frá því að slíkt innra eftirlit skuli viðhaft eða takmarkað til hvaða þátta í vinnslunni það skuli taka.

7. gr.

13. gr. laganna orðast svo ásamt fyrirsögn:

Trúnaðarskylda vinnsluaðila við meðferð persónuupplýsinga.

Ábyrgðaraðila er heimilt að semja við tiltekinn aðila um að annast, í heild eða að hluta, þá vinnslu persónuupplýsinga sem hann ber ábyrgð á samkvæmt ákvæðum laga þessara. Slíkt er þó háð því skilyrði að ábyrgðaraðili hafi áður sannreynt að umræddur vinnsluaðili geti framkvæmt viðeigandi öryggisráðstafanir og viðhaft innra eftirlit skv. 12. gr. laga þessara.

Samningur skv. 1. mgr. skal vera skriflegur og a.m.k. í tveimur eintökum. Þar skal m.a. koma fram að vinnsluaðila sé einungis heimilt að starfa í samræmi við fyrirmæli ábyrgðaraðila og að ákvæði laga þessara um skyldur ábyrgðaraðila gildi einnig um þá vinnslu sem vinnsluaðili annast. Ábyrgðaraðili og vinnsluaðili skulu hvor varðveita sitt eintak af samningnum.

Hverjum þeim er starfar í umboði ábyrgðaraðila eða vinnsluaðila, að vinnsluaðila sjálfum meðtöldum, og hefur aðgang að persónuupplýsingum, er aðeins heimilt að vinna með persónuupplýsingar í samræmi við fyrirmæli ábyrgðaraðila nema lög mæli fyrir á annan veg.

Hafi vinnsluaðili staðfestu í öðru ríki á Evrópska efnahagssvæðinu en ábyrgðaraðili, sbr. 1. mgr. 6. gr., skal jafnframt mælt svo fyrir í samningi að lög og reglur þess ríkis þar sem vinnsluaðili hefur staðfestu gildi um öryggisráðstafanir við vinnslu persónuupplýsinga. Getur Persónuvernd t.d. í auglýsingu í Stjórnartíðindum áskilið að slíkur samningur innihaldi stöðluð ákvæði sem séu í samræmi við ákvörðun framkvæmdastjórnar Evrópubandalagsins. Sama á við þegar ábyrgðaraðili hefur staðfestu í ríki á Evrópska efnahagssvæðinu en vinnsluaðili ekki fari vinnslan fram í landi eða á stöðum sem upp eru taldir í auglýsingu sem Persónuvernd gefur út.

8. gr.

28. gr. laganna orðast svo ásamt fyrirsögn:

Um andmælarétt hins skráða og um bannskrá Hagstofunnar.

Hinum skráða er heimilt að andmæla vinnslu upplýsinga um sjálfan sig ef hann hefur til þess lögmætar og knýjandi ástæður vegna sérstakra aðstæðna sinna nema kveðið sé á um annað í öðrum lögum. Eigi andmælin rétt á sér er ábyrgðaraðila óheimil frekari vinnsla umræddra upplýsinga.

Hagstofa Íslands skal halda skrá yfir þá sem andmæla því að nöfn þeirra séu notuð í markaðssetningarstarfsemi, en Hagstofa Íslands setur nánari reglur um gerð og notkun slíkra skráa og hvaða upplýsingar skuli koma þar fram í samráði við Persónuvernd. Ábyrgðaraðilar sem starfa í beinni markaðssókn og þeir sem nota skrá með nöfnum, heimilisföngum, netföngum, símanúmerum og þess háttar eða miðla þeim til þriðja aðila í tengslum við slíka starfsemi skulu, áður en slík skrá er notuð í slíkum tilgangi, bera hana saman við skrá Hagstofunnar til að koma í veg fyrir að markpóstur verði sendur eða hringt verði til einstaklinga sem hafa andmælt slíku. Persónuvernd getur heimilað undanþágu frá þessari skyldu í sérstökum tilvikum.

Öll notkun bannskrár skv. 2. mgr. er óheimil í öðrum tilgangi en þar er lýst.

Skylt er að nafn ábyrgðaraðila komi fram á áberandi stað á útsendum markpósti og hvert þeir sem andmæla því að fá slíkan markpóst og marksímtöl geti snúið sér. Viðtakandi markpósts á rétt á að fá vitneskju um hvaðan þær upplýsingar koma sem liggja úthringingu eða útsendingu til grundvallar. Þetta gildir ekki um markaðssetningu ábyrgðaraðila á eigin vöru og þjónustu sem notar eigin viðskiptamannaskrár, enda beri útsent efni með sér hvaðan það kemur.

Ábyrgðaraðila er heimilt að afhenda félag-, starfsmanna- eða viðskiptamannaskrár til nota í tengslum við markaðssetningarstarfsemi. Þetta á þó aðeins við ef:

1. ekki telst vera um afhendingu viðkvæmra persónuupplýsinga að ræða,
2. hinum skráðu hefur, áður en afhending fer fram, verið gefinn kostur á að andmæla því, hverjum fyrir sitt leyti, að upplýsingar um viðkomandi birtist á hinni afhentu skrá,
3. slíkt fer ekki gegn reglum eða samþykktum viðkomandi félags,

4. ábyrgðaraðili kannar hvort einhver hinna skráðu hefur komið andmælum á framfæri við Hagstofuna, sbr. 2. mgr., og eyðir upplýsingum um viðkomandi áður en hann lætur skrána af hendi.

Ákvæði 5. mgr. gildir ekki ef afhending félaga-, starfsmanna- eða viðskiptamannaskrár til nota við dreifingu markpósts byggist á samþykki hins skráða, sbr. 1. tölul. 1. mgr. 8. gr.

Ákvæði 1.–5. mgr. gilda, eftir því sem við á, einnig um markaðs-, neyslu- og skoðanakannanir. Persónuvernd er heimilt að undanþiggja vísindarannsóknir og hliðstæðar rannsóknir slíku takmörkunum, enda þyki ljóst að slíkt geti skert til muna áreiðanleika niðurstöðu rannsóknarinnar.

9. gr.

Við 2. mgr. 29. gr. laganna bætist nýr málslíður, svohljóðandi: Sama á við um lönd eða staði sem Persónuvernd auglýsir í Stjórnartíðindum að virtum ákvörðunum framkvæmdastjórnar Evrópubandalagsins.

10. gr.

Eftirfarandi breytingar verða á 30. gr. laganna:

- a. Við 1. mgr. bætast tveir nýir töluliðir, svohljóðandi:
7. ef miðlun er nauðsynleg eða fyrirskipuð samkvæmt lögum vegna þess að brýnir almannahagsmunir krefjast þess eða til að unnt sé að stofna, hafa uppi eða verja réttarkröfur, eða
 8. um sé að ræða upplýsingar sem almennur aðgangur er að.
- b. Í stað lokamálsliðar 2. mgr. koma fjórir nýir málslíðir, svohljóðandi: Persónuvernd getur heimilað miðlun persónuupplýsinga til þriðju landa þótt þau hafi ekki verið talin veita friðhelgi borgaranna nægilega einkalífsvernd. Slíkt er háð því að ábyrgðaraðili hafi, að mati stofnunarinnar, veitt nægilegar tryggingar fyrir slíku. Getur stofnunin t.d. áskilið að ábyrgðaraðili hafi gert við viðtökuaðila skriflegan samning sem hafi að geyma tiltek-in stöðluð samningsákvæði í samræmi við ákvörðun sem Persónuvernd hefur auglýst í Stjórnartíðindum, að teknu tilliti til ákvarðana framkvæmdastjórnar Evrópubandalagsins, sbr. 2. mgr. 29. gr. laga þessara. Að öðru leyti getur Persónuvernd sett nánari fyrir-mæli um flutning persónuupplýsinga úr landi.

11. gr.

Við fyrri málslíð 2. mgr. 37. gr. laganna bætist: á Íslandi, hvort sem íslensk lög eða lög annars ríkis gilda um vinnsluna.

12. gr.

Lög þessi öðlast þegar gildi.

Samþykkt á Alþingi 20. maí 2001.