

Reykjavík, 25. ágúst 2023

Tilvísun: 2308069

Dómsmálaráðuneytið

Borgartúni 26

105 Reykjavík

Umsögn Sjúkratrygginga Íslands: Áform um breytingar á persónuverndarlögum.

Þann 18. júlí sl. voru kynnt í Samráðsgátt áform um breytingar á persónuverndarlögum. Meðfylgjandi er umsögn Sjúkratrygginga.

Sjúkratryggingar telja að bæta þurfi nálgun laganna gagnvart persónuverndarmálum opinberra aðila og gera leiðbeiningar- og stuðningshlutverk Persónuverndar hærra undir höfði, fremur en að áherslan beinist að eftirliti og refsingu eins og nú virðist vera. Ljóst er að sektarheimild Persónuverndar veldur alvarlegri skekkju í viðleitni opinberra stofnana til að fara að fjölmörgum kröfum löggjafar við starfsemi þeirra. Það getur ekki talist eðlilegt að afleiðingar brota á reglum um persónuvernd séu meira íþyngjandi en mögulegra brota á öðrum reglum sem opinberum aðilum ber að hlíta. Núverandi nálgun Persónuverndar í eftirliti og refsingu hvetji til áhættufælni og geta þannig haft neikvæð áhrif á viðleitni stofnana til að bæta stafræna þjónustu og efla upplýsingaöryggi. Þá er þörf að skýra eða breyta tilteknum ákvæðum laganna í ljósi núverandi framkvæmdar, sjá nánar í umfjöllun hér á eftir.

Umsögn vegna 23., 24. og 27. gr. laganna

Sjúkratryggingar telja mikilvægt að skýrt verði hvað falli undir *viðeigandi* tæknilegar og skipulagslegar ráðstafanir í ákvæðum 23., 24. og 27. gr. laganna. Ljóst er að núverandi framkvæmd er ekki í samræmi við orðalag ákvæðanna þar sem í ákvörðun Persónuverndar í máli 2020010085 kom fram að notkun gagna í prófunarumhverfi hafi ekki verið í samræmi við 24. gr. en ráðstöfun sem var beitt var í samræmi við stýringu 8.31 í ISO/IEC 27002:2022 sem er að öllu leyti viðeigandi. Rétt er að benda á að Persónuvernd taldi rétt að beita viðurlögum vegna þessa þrátt fyrir að ráðstöfun sem var í gildi væri í samræmi við viðurkennd viðmið innan upplýsingaöryggis. Með því að ganga lengra en orðalag laganna felur í sér, um *viðeigandi* ráðstafanir, eykst hættu á áhættufælni og getur slíkt leitt til stöðunar í nýsköpun og framþróun í upplýsingatækni.

Í leiðbeiningum evrópska persónuverndarráðsins um innbyggða og sjálfgefna persónuvernd frá október 2020¹ segir að ákvæði 25. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2016/679, frá 27. apríl 2016,

¹ Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020, bls 7, efnisgrein 14.

um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB sem kom til framkvæmda 25. maí 2018, setji ekki skyldu á ábyrgðaraðila til að innleiða *tilteknar* tæknilegar og skipulagslegar ráðstafanir, svo framarlega sem þær ráðstafanir sem í raun eru innleiddar séu *viðeigandi* fyrir þá vinnslu sem um ræðir.

Umsögn vegna 38. gr. laganna

Að mati Sjúkratrygginga væri rétt að innleiða málsskotsrétt til annarra en dómstóla vegna ákvarðana Persónuverndar. Sér í lagi er átt við ákvarðanir sem taka til meiri háttar efnislegra eða stefnumótandi ákvarðana sem tiltekin eru í liðum a-d í 3. mgr. 2. gr. reglna nr. 876/2017. Þegar aðili máls telur efnisannmarka eða brot á formsskilyrðum laganna vera til staðar við úrvinnslu mála hjá Persónuvernd og um er að ræða meiriháttar efnislegar og íþyngjandi ákvarðanir er nauðsynlegt að þessi réttur sé til staðar. Ljóst er að fæstir skjóta slíkum málum til dómstóla, vegna kostnaðar og óhagræðis. Þetta á einkum við um ákvarðanir Persónuverndar sem beinast að ríkisstofnunum. Eðli málsins samkvæmt þjónar það ekki tilgangi hins opinbera að standa í málaferlum við sjálft sig. Einnig getur ákveðinn freistnivandi verið fólgin í því að hafa ekki æðra úrskurðarvald á stjórnarsýslustigi.

Þá er nauðsynlegt að til staðar sé skýr heimild fyrir aðila máls að beina erindum að stjórn Persónuverndar vegna mála sem stjórnin tekur ákvörðun um, t.a.m. andmælum, beiðnum um endurupptöku og rökstuðning osfrv. Einnig þyrfti að skýra betur í ákvæðinu um hvenær það er Persónuvernd sem rækir hlutverk sitt og hvenær það er í höndum stjórnar Persónuverndar. Þetta væri til þess fallið að auka gagnsæi. Þá er óljóst hvað fellur undir *meiriháttar efnislegar ákvarðanir* í ákvæðinu þar sem um er að ræða huglægt mat.

Umsögn vegna 39. gr. laganna

Í 39. gr. kemur ekki fram að Persónuvernd framkvæmi frumkvæðisúttektir á upplýsingatækni og upplýsingaöryggi. Þá er ekki kveðið á um að Persónuvernd framkvæmi úttektir á heildarstarfsemi stofnana/fyrirtækja. Eðli málsins samkvæmt geta slíkar úttektir verið íþyngjandi og því mikilvægt að skýr heimild sé fyrir þeim í lögum. Ekki verður séð að slíkar úttektir falli undir 3. mgr. 39. gr., 23. og 24. gr. eða önnur ákvæði laganna. Þá verður ekki séð að i. liður 2. mgr. 4. gr. né ákvæði VII. kafla reglna nr. 1246/2021 feli í sér slíkar heimildir.

Þurfi Persónuvernd aðstoð sérfræðings við meðferð máls er eðlilegast að Persónuvernd beri kostnað af slíkri sérfræðivinnu en ekki sá málsaðili sem málið heyrir til. Því er lagt til að fella úr gildi 33. gr. reglna nr. 1246/2021.

Umsögn um 42. og 46. gr. laganna

Í ljósi núverandi framkvæmdar er ljóst að skýra þarf betur samspil 42. og 46. gr. laganna, áður en viðurlögum er beitt. Í 42. gr. ætti að koma fram hvaða framkvæmd skuli vera viðhöfð við athugun eða úttekt á einstöku máli við útgáfu fyrir mæla eða tilmæla um úrbætur og gefa viðeigandi tímafresti áður en viðurlögum er beitt. Þá ætti einnig að koma fram að Persónuvernd beri að taka tilliti til aðstæðna, kostnaðar og annarra atriða við útgáfu tilmæla, sjá 23. og 24. gr. og umfjöllun hér að framan um orðalagið *viðeigandi* ráðstöfun.

Í ljósi þróunar núverandi framkvæmdar er mikilvægt að stjórnvöld og ríkisstofnanir verði undanþegin 46. gr. Sjúkratryggingar benda á sérstöðu þess að íslenskt stjórnvald hafi lagaheimildir til að beita annað stjórnvald stjórnvaldssektum og minna á að aðildarríkjum ESB og samningsaðilum EES svæðisins var með hinni almennu persónuverndarreglugerð ESB nr. 2016/679 (GDPR) veitt sjálfdæmi um hvort þeir tækju upp slíka tilhögun, sjá 7. tölulið 83. gr. GDPR. Um opinbera aðila sem hafa lögboðnar skyldur til vinnslu persónuupplýsinga gildir í langflestum tilvikum að sérlega nauðsynlegt er að starfsemi þeirra njóti trausts. Beiting sektarheimildar af hálfu Persónuverndar er til þess fallin að rýra það traust. Í þessu samhengi vekja Sjúkratryggingar athygli á afstöðu bresku persónuverndarstofnunarinnar, Information Commissioner's Office (ICO) til sektarálagningar, sér í lagi í málum er varða opinberar stofnanir. Í auknum mæli hefur ICO fallið frá sektarálagningum á opinbera aðila þar sem í henni felist óhagkvæm færsla fjármuna milli opinberra aðila og þar sem stofnunin telur önnur framfylgdarúrræði betur til þess fallin að ná árangri og gæta að vernd borgaranna.²

Umsagnir um ákvæði sem vantar í lög

Í lögum vantar ákvæði um hvernig gagnamiðlun skuli fara fram með öruggum hætti er varðar málsmeðferð hjá Persónuvernd, sambærilegt ákvæði og í 50. gr. laga nr. 112/2008 um sjúkratryggingar.

Skýra þarf betur í lögum um rétt málsaðila til að fá upplýsingar um ástæður fyrir rannsókn eða úttekt, þ.e. hvað kom fram í kvörtun/ábendingu. Það er mikilvægt að þetta verði innleitt til að aðilar geti nýtt andmælarétt sinn áður en til ákvörðunar Persónuverndar kemur.

Einnig er mikilvægt að í lögum komi fram tímamörk varðandi úttektir og athuganir þannig að málsaðilar sæti ekki íþyngjandi ráðstöfunum í lengri tíma, sbr. mál nr. 2020010085.

² Afstaða ICO kemur skýrlega fram í ávarpi forstjóra ICO á NADPO (National Association of Data Protection Officers) ráðstefnunni, þann 22. nóvember 2022: [How the ICO enforces: a new strategic approach to regulatory action](https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/11/how-the-ico-enforces-a-new-strategic-approach-to-regulatory-action/), aðgengilegt á <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/11/how-the-ico-enforces-a-new-strategic-approach-to-regulatory-action/>

Virðingarfyllst, f.h. Sjúkratrygginga
Kristján Þorvaldsson, sviðsstjóri Upplýsingatæknisviðs
Elsa Gísladóttir, persónuverndarfulltrúi

Undirritunarsíða

sviðsstjóri Upplýsingatæknisviðs
Kristján Þorvaldsson



Undirritað af:
Kristján Þorvaldsson
0802833699
Dags: 25.08.2023
Tími: 16:00:19
Ástæða: Samþykkt
Signet ID: f31721ef-7fe8-
4627-aa22-cfad98832724

persónuverndarfulltrúi
Elsa Rún Gísladóttir



Undirritað af:
Elsa Rún Gísladóttir
0501833439
Dags: 25.08.2023
Tími: 16:38:49
Ástæða: Samþykkt
Signet ID: f31721ef-7fe8-
4627-aa22-cfad98832724