Nefndarsvið Alþingis

Allsherjar- og menntamálanefnd

Kaupmannahöfn 5. júní 2018

Efni: Umsögn um frumvarp til laga um persónuvernd og vinnslu persónuupplýsinga á þingskjali 1029.

Undirritaður óskar eftir að koma á framfæri við allsherjar- og menntamálanefnd eftirfarandi upplýsingum og athugasemdum.

Undirritaður hefur unnið sem öryggisstjóri og ráðgjafi í tengslum við persónuvernd og meðferð persónuupplýsinga frá haustdögum árið 1997. Hef ég m.a. veitt nánast öllum lífeyrissjóðum landsins ráðgjöf vegna núgildandi laga, fjölda annarra fjármálafyrirtækja og Íslenskri getspá á Íslandi, APMM og Moderniseringsstyrelsen í Danmörku, Sykerhuspartner í Noregi og Nokia í Finnlandi, svo nokkrir aðilar séu nefndir. Vegna persónuverndarreglugerðarinnar, sem þessu frumvarpi er ætlað að veita lagastoð, hef ég veitt undirstofnun danska fjármálaráðuneytisins (Moderniseringsstyrelsen), 150 grunnskólum á Íslandi aðstoð, auk minni verkefna víða í Evrópu. Hef ég því bæði umfangsmikla þekkingu á núverandi lögum, hef nýtt hana í minnst fjórum löndum, auk þess að hafa reynslu af innleiðingu reglugerðarinnar nr. 2016/679.

Frumvarpið sem hér um ræðir er seint komið fram og því er stillt upp af ráðherra, sem nánast óumbreytanlegu. Ég viðurkenni að reglugerðinni verði ekki breytt, en frumvarpinu er bæði hægt að breyta og nauðsynlegt að breyta a.m.k. þeim greinum sem ég nefni að neðan.

Fyrst vil ég nefna, að frumvarpið á þingskjali 1029, er að mörgu leyti mjög ólíkt nýlega samþykktum dönskum lögum, sem finna má á slóðinni: https://www.retsinformation.dk/Forms/R0710.aspx?id=201319. Skýringuna á mismuninum má finna í mismunandi aðferð við lagasetningu í þessum tveimur löndum. Þetta hins vegar segir, að Alþingi getur breytt texta frumvarpsins, ef svo ber undir.

Athugasemdir við einstakar greinar

1. gr. Markmið

Erfitt er að sjá, að það sé hluti af markmiðum laganna, að sérstök stofnun, Persónuvernd, annist eftirlit, eins og segir í 2. málsgrein (efnisgrein). Málsgreinin kemur raunar ekki markmiðum laganna við, heldur lýsir framkvæmd. Lagt er til að málsgreinin sé flutt til innan laganna og verði hluti af nýrri 38.gr. í VII. kafla, en greinar þar fyrir aftan verði færðar niður. VII. kafli fjallar um eftirlit og því rangt að tilgreina undir Markmið að Persónuvernd hafi eftirlit.

Tillaga að breytingu:

Í frumvarpið komið ný 38.gr. og aðrar greinar færist neðar sem því nemur:

38.gr. hljóði svo:

38.gr. Eftirlitshlutverk Persónuverndar

Sérstök stofnun, Persónuvernd, annast eftirlit með framkvæmd reglugerðar Evrópuþingsins og ráðsins (ESB) 2016/679, laga þessara og reglna sem settar verða samkvæmt þeim, sbr. nánar ákvæði VII. kafla laga þessara. Evrópsk eftirlitsstofnun skv. VII. kafla reglugerðarinnar er Evrópska persónuverndarráðið.

4.gr. Efnislegt gildissvið

Réttur látins einstaklings og aðstandenda

Í 3. málsgrein (efnisgrein) eru settar takmarkanir á að lögin og reglugerðin gildi eingöngu um persónuupplýsingar í 5 ár eftir andlát. Reglugerðin leggur það í hendur hvers þjóðþings að ákveða hve lengi fólk nýtur friðhelgi eftir andlát. Danir fóru þá leið að hafa þennan tíma 10 ár (grein 2, liður 5). Fimm ár er mjög stuttur tími, auk þess sem friðhelgiupplýsingar tengjast mjög oft eftirlifandi ættingjum. Raunar eru 10 ár einnig stuttur tími, en þó skömminni skárri en fimm ár. Er lagt til að lögin nái yfir persónuupplýsingar í 10 ár eftir andlát, en þingmenn hugleiði að setja þetta jafnvel upp í 15 ár.

Bið ég þingmenn um að setja sig í spor eftirlifanda eins og einhver nákominn hafi fallið frá. Eftir 5 ár, er sá sem liggur með upplýsingarnar allt í einu ekki bundinn af því að eyða þeim í samræmi við ákvæði laganna, þrátt fyrir að viðkomandi aðili hafi engar efnislegar ástæður fyrir því að geyma þær. Af hverju eiga látinn einstaklingur og aðstandendur hans að hafa minni vernd, þegar kemur að tilgangslausri vörslu persónuupplýsinga hins látna? Það sem gerir það einnig mikilvægt að miða við 10 ár, ef ekki þess vegna lengri tíma, eru ákvæði um fyrningar, bókhaldslög og skattalög. Fjármálafyrirtæki hafa t.d. ekkert að gera með að varðveita allar upplýsingar um látna viðskiptavini sína löngu eftir andlát. 5 ára reglan leggur það alfarið í hendur þessum fyrirtækjum í hve langan tíma þau geyma þessar upplýsingar, þar sem önnur lög skylda þau að geyma upplýsingarnar að lágmarki í 7 ár. Ákvæðið er því marklaust hvað kemur að því að vernda hinn látna og aðstandendur viðkomandi. (Verndin gagnvart aðstandendum, sem ég er að vísa til, er fyrst og fremst að þurfa að búa við að þarflausar upplýsingar um látinn fjölskyldumeðlim séu að birtast löngu eftir andlát, einfaldlega vegna þess að ábyrgðaraðili upplýsinganna þurfti ekki að eyða þeim eða verja með tilhlýðilegum hætti.)

Þetta atriði snýst fyrst og fremst um, að ábyrgðaraðilar upplýsinga um látna einstaklinga geti ekki geymt þær upplýsingar út í það óendanlega, meðan þeir þurfi að eyða upplýsingum um lifandi einstaklinga eftir t.d. 7 ár. Réttur lifandi og látinna á að vera sá sami hvað varðar þennan þátt. Annað er, að aðstandendur látins einstaklings eiga að hafa rétt á að vita hvaða upplýsingar eru varðveittar um viðkomandi, geta krafist þess að úreltar upplýsingar séu leiðrétta, við þær bætt eða þeim eytt. Þessi réttur fellur niður eftir 5 ár, eins og 3. mgr. 4.gr. frumvarpsins hljómar.

Í athugasemdum með frumvarpinu kemur fram, að mörkin hafi verið 10 ár, en þau færð í 5 ár að áeggjan samtaka fyrirtækja í atvinnulífinu. Ég get alveg skilið, að þessi samtök vilji hafa mörkin við 5 ár, því þá þurfa þau ekki að hafa áhyggjur af því að hreinsa til í gagnasöfnum sínum. Bókhaldslög og skattalög krefjast að þau geymi t.d. viðskiptasögu einstaklinga í ýmist 6 eða 7 ár, en þessi fyrirtæki miða almennt við, þegar viðskiptavinur hefur sannanlega hætt viðskiptum. Ljóst er því, að með þessum mörkum eiga lögin einfaldlega ekki að skylda fyrirtæki til að taka til í gagnasöfnum sínum.

Síðan þarf að skýra betur út hver kemur fram fyrir hönd hins látna gagnvart lögunum. Þess er hvergi getið og skilur það því eftir lagalegt tómarúm. Það er nefnilega þannig, að hinn látni mun ekki geta lagt sjálfur fram óskir um að gleymast, andmælt vinnslu persónuupplýsinga, leiðréttingu á röngum upplýsingum, o.s.frv. Það geta hins vegar verið ríkar ástæður fyrir slíkum óskum fyrir hönd hins látna, svo sem atriði er lúta að mannorði viðkomandi og rangar upplýsingar í ættfræðiritum, svo tvö dæmi séu tekin.

Það er alveg út í hött, að láta undan þrýstingi frá þeim sem stunda söfnun persónuupplýsinga (oft án nokkurs samþykkis hins skráða), að gera stóran hluta persónuverndar látinna einstaklinga að engu með því að stytta tímann í 5 ár. Þá er alveg eins hægt að fara norsku leiðina og láta lögin og reglugerðina ekki ná yfir látna einstaklinga.

Ég legg til að miðað verði við 10 ár og að jafnframt verði skýrt betur hverjir geta komið fram fyrir hönd hins látna.

Tillaga að breytingu:

3. mgr. 4.gr. hljóði sem hér segir:

> Lög þessi og reglugerðin gilda um vinnslu persónuupplýsinga látinna einstaklinga í 10 ár frá andláti þeirra en lengur þegar um ræðir persónuupplýsingar sem sanngjarnt og eðlilegt má telja að leynt fari. Nánir ættingjar hins látna geta gætt réttinda hins látna í samræmi við ákvæði þessara laga og reglugerðarinnar.

18. gr. Verndarráðstafanir og undanþágur varðandi vinnslu vegna rannsókna, tölfræði eða skjalavistunar í þágu almannahagsmuna.

Eins og ég kom að í upphafi umsagnarinnar, þá hef ég verið að veita GDPR ráðgjöf fyrir Moderniseringsstyrelsen hér í Danmörku. Þar tókum við m.a. umræðu um atriði sem skipti miklu máli varðandi vernd persónuupplýsinga, en það er þessi skylda opinberra aðila að skila skjölum til opinberra skjalasafna. Meðan á Íslandi er nánast öllu skilað, þá hafa Danir skorið þessi skil mikið niður.

Ansi mikið af upplýsingum hefur ekkert að gera með að vera sent til opinbers skjalasafns, þar sem nánast allir geta haft aðgang að þeim. Tala nú ekki um, þegar vernd persónuupplýsinga á að falla niður eftir 5 ár, eins og segir í frumvarpinu. Þessari óhóflegu söfnun persónuupplýsinga hjá opinberum skjalasöfnun verður að ljúka. Fyrsta skrefið er að láta væntanleg persónuverndarlög ná til viðkvæmra persónuupplýsinga opinberra aðila hvað varðar varðveislu upplýsinganna og eyðingu.

Viðkvæmar persónuupplýsingar eiga EKKERT erindi inn á opinbert skjalasafn. Það er gamli tíminn. Þessi regla hefur áhrif á upplýsingaskráningu t.d. grunnskóla, sem veigra sér við að halda utan um jafnvel nauðsynlegar upplýsingar, vegna þess að þær munu 10 árum eftir að skólagöngu nemandans lýkur enda inn á opinberu skjalasafni. Hefði Jón Sigurðsson eða Hannes Hafstein komist í þangað sem þeir komust, ef lesa hefði mátt um það á ríkisskjalasafni að þeir hefðu verið ódælir í æsku, átt uppstökkar mæður og áhugalausa feður (allt tilbúningur). Núna er þetta ofvirkni, athyglisbrestur, skapstór, leti, og skróp, fyrir utan alla sjúkdómana. Þetta kemur bara engum við í framtíðinni og þessu verður að linna.

Núna er tækifærið og það felst í því að breyta fyrstu málsgrein 5.gr. Tengsl við önnur lög, þannig að vernd og vinnsla viðkvæmar persónuupplýsinga skuli alltaf falla undir ákvæði þessara laga. Það þýðir m.a. að þeim skuli eytt, þegar tilgangur söfnunar þeirra er ekki lengur til staðar. Sem sagt, þær skuli EKKI senda persónugreinanlegar á opinber skjalasöfn.

Þessi breyting kallar á að lögum 77/2014 um opinber skjalasöfn þurfi að breyta, þannig að þau taki ekki við nákvæmum lýsingum á viðkvæmum atriðum, sem skráð hafa verið t.d. í sjúkraskrá, greiningarskýrslur, nemendaskrá skóla, o.s.frv. Hvað kemur það framtíðinni við að Jón Jónsson hafi fallið í almennri lögfræði í fyrstu tilraun hans til að ná prófinu, þegar það eina sem skiptir máli er að hann lauk embættisprófi í lögfræði árið 19xx? Eða að þegar Guðrúnu Jónsdóttur var nauðgað 17 ára

gamalli árið 20xx, þá var hún neydd til endaþarmsmaka? Eða að Sigurður Jónsson, sem haldinn var alvarlegum kvíða, hafi reynt að svipta sig lífi í kvíðakasti árið 20xx?

Það er í mínum huga glatað tækifæri, að innleiða ný persónuverndarlög með nýrri hugsun, þegar halda á inni hátt í 150 ára hugsunum um hömlulausa söfnun upplýsinga hjá opinberum skjalasöfnum.

Tillaga að breytingu:

Síðasta málsgrein 18.gr. hljóði sem hér segir:

> Heimilt er að afhenda opinberu skjalasafni almennar persónuupplýsingar sem falla undir lög þessi í samræmi við ákvæði laga um opinber skjalasöfn. Eingöngu er heimilt að afhenda viðkvæmar persónuupplýsingar að ítarlegar og/eða meiðandi lýsingar hafi verið fjarlægðar.

46. gr. Stjórnvaldssektir

Í greininni er tilgreint að stjórnvaldsektir geti verið á milli tveggja upphæða. Annars vegar 100 þús. til 1,2 milljarðar kr. og hins vegar 100 þús. til 2,4 milljarðar kr. Reglugerðin setur hins vegar engin neðri mörk og því undarlegt, að það sé gert í íslensku lögunum. Hafa verður í huga, að mjög líklega mun fara í gang æði eftir gildistöku laganna, þar sem einstaklingar munu leita uppi alls konar atriði sem hafa farið úrskeiðis. Þessi atriði munu finnast, vegna þess að vitund fyrirtækja og stofnana fyrir persónuvernd hefur verið frekar takmörkuð. Með því að setja neðri mörk, þá gæti Persónuvernd neyðst til, vegna fyrri fordæma, að leggja margfaldar 100.000 kr. sektir á fyrirtæki og stofnanir. Slíkt hleypur fljótt á milljónum. Ég legg til að neðri mörk stjórnvaldssektanna verði felld niður í báðum tilfellum og það alfarið lagt í hendur Persónuverndar að ákvarða sektarfjárhæð.

Tillaga að breytingu:

> Í 2. og 3.mgr. falli niður orðin „frá 100 þús. kr. til“, en í staðinn komi „allt að“.

47. gr. Atriði sem áhrif hafa á ákvörðun um stjórnvaldssektir

Þessi grein virðist vera heimasmíði, a.m.k. fann ég ekki beina tilsvörun fyrir henni í reglugerðinni, enda er þetta mál sem 29. gr. hópurinn svo kallaði hefur verið að fjalla um. Það er mín skoðun, að þarna vanti inn atriði til málsbóta fyrir ábyrgðaraðila/vinnsluaðila. Í síbreytilegum heimi eru nánast daglega að koma fram upplýsingar um nýja veikleika í kerfum, nýja tækni til innbrota og svo má ekki gleyma, að engin tækni er þess fyrir utan örugg. Það er ekki til 100% öryggi sama hvað við reynum. Hvorki færustu sérfræðingar né bestu eftirlitsaðilar hafa tök á að fylgjast með öllu sem er að gerast. „Fullkomin“ tækni sem innleidd var í gær, gæti verið úrelt á morgun. Hvernig á það að skipta máli, að aðili hefur fylgt fyrirmælum Persónuverndar (sbr. liður 9), þegar þau fyrirmæli voru jafnvel röng eða byggð á ófullkominni þekkingu. Þó ég þekki persónulega marga af helstu sérfræðingum þjóðarinnar í upplýsingaöryggismálum og telst líklegast sjálfur til þess hóps, þá dettur mér ekki í hug að þeir (eða ég) hafi nægilega þekkingu til að veita 100% rétt fyrirmæli. Þess vegna verður þessi þáttur að snúast um áhrifamatið (mat á áhrifum á persónuvernd – MÁP, sbr. 29.gr.) sem gerð er krafa um. Taka verður tillit til þess hvernig aðilar unnu úr þessu áhrifamati, hvaða fjárhagslega burði þeir höfðu til að kaupa og innleiða bestu lausnir, hvernig þeir meðhöndluðu umframáhættu, hvort sú meðhöndlun var réttlætanleg og hvort líklegt er að niðurstaðan hafi verið í samræmi við bestu starfsvenjur. Hugsanlega er hægt að túlka að 4. liður dekki þetta, en hann gerir það ekki, vegna þess að hann vísar ekki til formálsgreina (e. recitals) reglugerðarinnar. 25. gr. og 32. gr. reglugerðarinnar vísa ekki sjálfstætt í formálagreinarnar, heldur þarf verulega þekkingu til að átta sig á hvaða formálsgreinar eiga við. Hvað þessar greinar varðar, þá eru það formálsgreinar 75 (Áhætta vegna

réttinda og frelsis einstaklings), 76 (Áhættumat), 77 (Leiðbeiningar um áhættumat), 78 (Viðeigandi tæknilegar og skipulagslegar ráðstafanir), 79 (Úthlutun ábyrgða) og 80 (Öryggi vinnslu) (greinarnar bera ekki sérstakt heiti í reglugerðinni, en þær ganga almennt undir þessum – þýðing úr ensku er mín) og þá sérstaklega nr. 78. Það er tómt mál að vísa til gr. 25 og 32 án þess að vísa í þessar formálsgreinar líka og jafnvel 35.gr. reglugerðarinnar, sem fjallar um mat á áhrifum á persónuvernd.

Svona til að taka þetta saman, þá finnst mér vanta í 47.gr. nákvæmari tilvísun í fagleg vinnubrögð allra, þá sérstaklega að áhættumat/áhrifamat sé notað til að meta hvað telst vera eðlilegar öryggisreglur/-kröfur sem ábyrgðaraðili og vinnsluaðili innleiða.

Stærsta hættan við margt í 47.gr. er að fyrirtæki og stofnanir fari að leita í miklu mæli til Persónuverndar um samþykki fyrir því fyrirkomulagi öryggis persónuupplýsinga, sem hefur verið innleitt. Nokkuð sem Persónuvernd hefur enga burði til að standa í, þrátt fyrir að stofnunin sé að bæta við sig hæfum einstaklingum. Nú vottunaraðilar skv. 42.gr. reglugerðarinnar verða ekki til staðar í bráð og þeir munu líka vera í óvissu um hvað telst vera öruggt. Þess vegna verður áhrifamatið

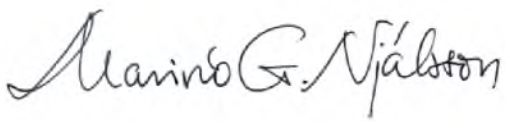
Öryggisbrestir munu verða, sama hvað, en það verður að vera öruggt, að þeir sem virkilega lögðu sig fram við að byggja gott öryggiskerfi, verði ekki kjöldregnir í sektarákvörðunum, vegna þess að þeir vissu ekki af öllum veikleikum kerfanna sinna, sem hins vegar einhverjir tölvuþrjótar vissu af.

Vil ég svo benda á, að í nýlegu máli er varðar skóla á Norðurlandi, þá virðist Persónuvernd leggja gríðarlegar kröfur á skólann að kanna öryggiskerfi stærsta tölvuhýsingarfyrirtækis landsins. Skólinn mátti ekki treysta öryggisvottun fyrirtækisins, að það sér um hýsingu fyrir mörg stærstu fyrirtæki landsins og opinberar stofnanir, að fyrirtækið gefur sig út fyrir að vera með öll sín mál á hreinu. Nei, skólinn átti að hafa ítarlega þekkingu á kröfum, sem eru ekki á allra vitorði, senda hýsingaraðila opinberra stofnana til margra áratuga þessar kröfur og óska eftir skriflegum svörum. Ég er ekki viss um hvort sá sem útbjó svar Persónuverndar hafi áttað sig á því, að ekki var nóg fyrir stofnunina að óska eftir þessu við þennan litla skóla á Norðurlandi, heldur þyrfti stofnunin núna að senda sambærilega ábendingu/kröfu til allra fyrirtækja og opinberra stofnana með hýsingu hjá viðkomandi hýsingaraðila, því umrætt öryggisbrot varð hjá hýsingaraðilanum. Eigi jafnræðisregla stjórnsýslunnar að gilda, þá varðaði þetta öryggisbrot alla viðskiptavini fyrirtækisins, þó það hefði bara afleiðingar fyrir einn.

Tillaga að breytingu:

> Við 4. lið 47.gr. bætist: „og í samræmi við niðurstöður mats á áhrifum á persónuvernd skv. 35.gr. reglugerðarinnar“

Með von um góðar undirtektir.



Marinó G. Njálsson

oryggi@internet.is

Sími: 898-6019 (íslenskt númer)