



RÍKISLÖGREGLUSTJÓRI

Reykjavík 19. ágúst 2022

Tilvísun: 2022060158

Fjármála- og efnahagsráðuneyti
Lindargötu Arnarhvoli
101 Reykjavík

Umsögn við mál nr. 103/2022 um öryggisflokkun gagna íslenska ríkisins

Almennt

Vísað er til máls nr. 103/2022 sem birt var á Samráðsgátt stjórnvalda þann 21. júní 2022, um öryggisflokkun gagna íslenska ríkisins. Embætti ríkislögreglustjóra telur mikilvægt af þessu tilefni að koma neðangreindum athugasemdum við skjalið á framfæri en jafnframt fagna því að þessi vinna við að móta heildstæða stefnu um öryggisflokkun gagna ríkisins sé hafin. Í athugasemdum er vísað til kaflaheita í skýrslu.

Rétt er að taka fram að hér er um að ræða framfaraskref með tilkomu skýrslunnar og fyrirhugaðrar vinnu varðandi öryggisflokkun gagna íslenska ríkisins sem embætti ríkislögreglustjóra telur vera til hagsbóta fyrir starfsmenn ríkisins og almenning. Af því leiðir að miklir hagsmunir eru í húfi að leiðbeiningarnar þjóni tilgangi sínum einkum hvað varðar skýrleika.

Ábendingar ríkislögreglustjóra við skýrslu fjármála- og efnahagsráðuneytisins um öryggisflokkun gagna íslenska ríkisins

Samantekt

Í samantekt eru skilgreindir fjórir öryggisflokkar. Er það mat embættis ríkislögreglustjóra að „Afmörkuð gögn“ sé ekki lýsandi heiti yfir öryggisflokk af hæstu gráðu og leggur eftirfarandi til. Það er mat embættisins að neðangreind tillaga að breyttri flokkun endurspegli betur stöðu gagna í hverjum flokk og sé lýsandi fyrir hversu viðkvæm gögn í hverjum flokki eru.

Núverandi flokkaheiti
Opin gögn
Varin gögn
Sérvarin gögn
Afmörkuð gögn

Tillaga að breyttri röðun flokkaheita
Opin gögn
Afmörkuð gögn
Varin gögn
Sérvarin gögn

Tillaga ríkislögreglustjóra: *Breytt uppröðun á flokkaheitum.*

3. Umfang

Í 3. kafla sem ber heitið Umfang segir „Leiðbeiningar þessar ná þannig til aðila sem búa til, safna, varðveita eða koma að vinnslu gagna sem eru hluti af stjórnsýslu ríkisins“. Er það mat embættis ríkislögreglustjóra að meðhöndlun gagna skv. skýrslunni skuli jafnframt ná til raunlægra (e.

physical) sendinga gagna, svo sem boðsendingar sem oft eru framkvæmdar af þriðja aðila. Þá ber jafnframt að vernda upplýsingar við munnlega miðlun þeirra, svo sem við hverja og í hvaða umhverfi innihald öryggisflokkaðra upplýsinga er rætt, allt eftir hvaða flokki þær tilheyra. Því leggur ríkislögreglustjóri til að ákvæði um aðra meðhöndlun gagna verði bætt við setningu.

Tillaga ríkislögreglustjóra: *Leiðbeiningar þessar ná þannig til aðila sem búa til, safna, varðveita eða koma að vinnslu og annarri meðhöndlun gagna sem eru hluti af stjórnsýslu ríkisins.*

4. Viðmið

Ákvæði um viðeigandi kröfur eru matskennd sem stuðlar vart að samræmdu verklagi. Þörf er á ákvæðum í löggjöf um lágmarkskröfur, ábyrgðar- og eftirlitsaðila. 4. kafli fjallar um viðmið í tengslum við þróun og gerð öryggisflokkanar gagna m.a. til leiðsagnar um rétta meðferð og flokkun þeirra. Í kaflanum er m.a. kveðið á um viðeigandi og gagnsæja meðferð og viðeigandi öryggisúræði, sem og viðeigandi kunnáttu í vörslu, umsýslu og öryggi gagnanna. Embætti ríkislögreglustjóra leggur áherslu á mikilvægi þess að viðmiðin verði skýr og formfest svo tryggja megi samræmt verklag og skilning á þeim viðmiðunarkröfum sem settar verða, ella er hætt á að viðmiðin verði matskennd og huglæg hverju sinni, sem og að framkvæmd verði mismunandi af þeim sökum.

5. Áherslur

Í 5. kafla er farið yfir fimm megináherslur sem lýsa nálgun og veita leiðsögn um útfærslu flokkunarkerfisins og notkun þess. Í málsgrein 5.2 er kveðið á um að öryggi gagna sé tryggt á viðeigandi hátt. Líkt og í athugasemdum við 4. kafla um viðmið hér að ofan, ítrekar embætti ríkislögreglustjóra mikilvægi þess að sameiginlegar lágmarkskröfur sem stofnanir þurfa að uppfylla verði formfestar svo tryggja megi samræmt verklag, túlkun og útfærslu á “viðeigandi” öryggisúræðum svo þau verði ekki matskennd og huglæg hverju sinni.

Í sömu málsgrein eru m.a. taldar upp “Þjóðaröryggislegar ógnir og afleiðingar”. Að mati embættisins verður að tryggja skýrari aðskilnað á slíkum þjóðaröryggislegum ógnum og afleiðingum varðandi meðferð upplýsinga. Annars vegar m.t.t. þessara leiðbeininga og hins vegar regluverks í tengslum við öryggis- og varnarmál þ.e. á grundvelli varnarmálalaga nr. 34/2008 og reglugerðar nr. 959/2012 um um vernd trúnaðarupplýsinga, öryggisvottanir og öryggisviðurkenningar á sviði öryggis- og varnarmála. Starfsmenn ættu aldrei að vera í vafa um hvort regluverkið gildir um meðferð upplýsinganna.

Það er mat embætis ríkislögreglustjóra að reglur um lágmarksöryggiskröfur og -ráðstafanir þurfi að lögfesta eða setja í reglugerð með stoð í lögum, svo tryggja megi samræmt og kerfisbundið verklag og þar með verndarstig upplýsinga innan stjórnsýslunnar. Einnig þyrfti ákvæði um að forstöðumenn einstakra stofnana skuli fela ákveðnum starfsmanni s.k. öryggisfulltrúa, að bera ábyrgð á að lágmarksöryggiskröfum um meðferð öryggisflokkaðra upplýsinga sé framfylgt hjá stofnunum.. Ennfremur er lagt til að skilgreint verði stjórnvald sem gegni hlutverki eftirlitsstjórnvalds í þessu samhengi. Æskilegt væri að slík löggjöf tæki til eftirfarandi öryggismálaflokka:

- Mannauðsöryggi.
- Raunlægt öryggi.
- Skjala- og upplýsingaöryggi (skjalastjórn og meðferð).
- Öryggi tölvu- og samskiptakerfa (tölvuöryggi).
- Verktaka- og þjónustuöryggi.

Hlutverk embættis ríkislögreglustjóra sem öryggisstjórnvalds, sbr. reglugerð nr. 959/2012, er m.a. að framkvæma öryggisúttektir hjá stofnunum á grundvelli reglugerðarinnar. Í slíkum úttektum hefur ítrekað komið í ljós að stjórnendur og starfsmenn stofnana hafa afar ólíkar hugmyndir um það hvað telst öruggt, viðunandi og viðeigandi þegar kemur að öryggismálum. Samræmdu verndarstigi upplýsinga verður varla náð innan stjórnsýslunnar ef það er lagt í hendur hverrar stofnunar, jafnvel starfsmanna, að meta hvað sé viðeigandi öryggisúrræði hverju sinni.

6. Hlutverk og ábyrgð

Í kafla 6.3 er fjallað um notendur gagna hvar málsgreinin lýkur á „*Tilfallandi afhending eða notkun gagna út frá öðrum forsendum gera viðtakendur ekki að notendum gagna*“. Embætti ríkislögreglustjóra bendir á að þessi framsetning gerir ekki ráð fyrir að tilfallandi afhending eða notkun gagnanna út frá öðrum forsendum, geti í einhverjum tilfellum gert viðtakendur að notendum þeirra. Þó tilfallandi afhending geri viðtakendur almennt ekki að notendum gagnanna þá er það ekki algilt. Leggur embætti ríkislögreglustjóra til breytingu á orðalagi.

Tillaga ríkislögreglustjóra: *Tilfallandi afhending eða notkun gagna út frá öðrum forsendum gera viðtakendur **almennt** ekki að notendum gagna.*

7. Öryggisflokkun gagna

Í lok fyrstu málsgreinar 7. kafla um öryggisflokkun gagna segir: „*Of hátt öryggisstig flokkunar getur valdið óþörfum kostnaði, flækjustigi í vinnulagi og kerfum og þannig hamlað nýtingu gagnanna*“. Að mati embættis ríkislögreglustjóra hefur orðalagið „*Of hátt öryggisstig flokkunar*“ heldur óljósa merkingu og leggur til breytt orðalag.

Tillaga ríkislögreglustjóra: *Flokkun gagna í of háan öryggisflokk getur valdið [...]*

Í lok annarar málsgreinar segir m.a. „*Meta þarf hver mögulegur ávinningur ytri aðila er af uppljóstrun eða spillingu gagnanna og gera ráð fyrir að viðkomandi aðili sé reiðubúinn til að verja fjármunum og fyrirhöfn í réttu hlutfalli við þann ávinning*“. Embætti ríkislögreglustjóra bendir á að greinin einskorðast við ytri aðila sem geta hagnast af uppljóstrun eða spillingu gagna. Í raun gæti umrætt ákvæði einnig náð til núverandi jafnt sem fyrrverandi starfsmanna, verktaka og/eða þjónustuaðila svo eitthvað sé nefnt. Því leggur embættið til breytt orðalag svo ljóst megi vera að innri aðilar geti einnig uppljóstrað eða spillt gögnum.

Tillaga ríkislögreglustjóra: *Meta þarf hver mögulegur ávinningur getur hlotist af uppljóstrun eða spillingu gagnanna og gera ráð fyrir að viðkomandi aðili/aðilar séu reiðubúnir til að verja fjármunum og fyrirhöfn í réttu hlutfalli við þann ávinning.*

Í kaflanum „Hvenær skal meta viðkvæmnis- eða öryggisstig gagna?“ segir: „*Endurskoða þarf þessa skiptingu reglulega til að tryggja að umfang sé viðeigandi á hverjum tíma*“. Að mati ríkislögreglustjóra er þörf á skýrari útfærslu á kröfum um gildistíma öryggisflokkunar og endurmat, þ.e. hækkun, lækkun eða aflétting trúnaðar á þeim upplýsingum og gögnum sem hafa verið öryggisflokkuð. Mikilvægt er að slíkt endurmat sé á ábyrgð stofnanda skjals að notendum þess sé ekki heimilt að breyta öryggisflokkuninni nema í samráði við stofnandann. Að öllu jafna skulu upplýsingar og gögn, önnur en „opin gögn“, ekki vera öryggisflokkuð lengur en nauðsynlegt þykir. Endurmat á öðrum flokkum ætti að fara kerfisbundið fram og ekki síðar en á fimm ára fresti.

Tillaga ríkislögreglustjóra: *Stofnandi skjals skal endurmeta merkingar þeirra upplýsinga sem hann hefur öryggisflokkað m.t.t. hækkunar, lækkunar eða afléttingu trúnaðar. Það skal gert reglulega þó aldrei sjaldnar en á fimm ára fresti. Ekki er heimilt að breyta öryggisflokkun eða aflétta trúnaði á upplýsingum í eigu annara stofnana, án þeirra samþykkis.*

Í kafla 7.1 undir „Skilgreiningar flokka“ er á bls. 11 ákvörðunartré/tafla með skýringum á skilgreiningum öryggisflokka fjögurra. Í töflunni kemur fram í skilgreiningu á „afmörkuð gögn“ „*Veldur uppljóstrun, leki eða tap samféluginu eða ríkinu stórfelldum skaða eða álitshnekki á alþjóðavísu EDA bresti í þjóðaröryggi*“. Ríkislögreglustjóri ítrekar í því samhengi athugasemd sem gerð var við 5. kafla, þ.e. að tryggja þarf að gögn sem trúnaðarflokkuð eru á grundvelli öryggis og varnarmála sbr. varnarmálalög og reglugerð nr. 959/2012 (t.d. NATO eða ESB) séu skýrt aðskilin frá gögnum er varða þjóðaröryggi sbr. leiðbeiningar þessar. Starfsmönnum þarf að vera ljóst, öllum stundum, hvort regluverkið á við sem þeir þurfa að uppfylla.

Tillaga ríkislögreglustjóra: *Auðveldi þarf notendum skilning á hvenær verklag um þjóðaröryggi gildir skv. íslenskri stjórnsýslu og hvenær verklag um öryggis- og varnarmál gildir.*

Hvað varðar kafla 7.2, þá er bent á að skilgreiningar skortir í tengslum við lágmarksöryggiskröfur og mat á hæfni og getu. Í kafla 7.2 er tafla yfir viðmið varðandi vistunarstaði gagna. Undir “Staðsetning vistunar” segir „*Ríkisaðili getur talist hæfur að uppfylla öryggiskröfum*“. Bent er á að um er að ræða tilvísun í óskráðar öryggiskröfur. Svo tryggja megi kerfisbundið og samræmt öryggi við vistun öryggisflokkaðra gagna þvert á stjórnsýslu þurfa lágmarksöryggiskröfur, sem notendum bera að uppfylla, að vera skýrar og aðgengilegar. Þær þurfa að vera samræmdar hvar miðlægt stjórnvald hefur það hlutverk að tryggja eftirlit með að lágmarkskröfunum sé framfylgt. Lokamálsgrein kafla 7.2 varðar m.a. mat á hæfni og getu vinnslu- og vistunaraðila út frá ýmsum sjónarmiðum. Hér ítrekast að lágmarkskröfur um mat á hæfni og getu þurfa að liggja fyrir svo vinnslu- og vistunaraðilum sé unnt að taka afstöðu til þeirra.

8. Viðmið og meðhöndlun

Í 8. kafla er tafla yfir viðmið og meðhöndlun. Embætti ríkislögreglustjóri gerir athugasemdir við eftirfarandi reiti töflunnar.

Afmörkuð gögn.

Meðferð trúnaðarupplýsinga á grundvelli öryggis- og varnarmála fellur ekki undir þessar leiðbeiningar.

Í reitunum „Afleiðing uppljósturnar“ og “Endurmat flokkunar” er annars vegar vísað til laga um varnarmál nr. 34/2008 og hins vegar til reglugerðar nr. 959/2012, sem sett er á grundvelli varnarmálalaga. Ríkislögreglustjóri gerir athugasemd við slíkar tilvísanir í ljósi þess að upplýsingar og gögn sem eru trúnaðarmerkt samkvæmt ákvæðum varnarmálalaga og reglugerðar nr. 959/2012 bera annars konar trúnaðarmerkingar en skilgreindar eru í þessum leiðbeiningum. Þær eru flokkaðar út frá alþjóðlegu flokkunarkerfi sem er byggt á annars konar skaðamati.

Bent er á að um meðhöndlun og aðgangsheimildir slíkra upplýsinga gildir ófrávíkjanlegt alþjóðlegt regluverk sem aðildar-/samningsríkin, þ.á m. Ísland hafa undirgengist og ber hlíta öllum stundum. Því telur embætti ríkislögreglustjóri ekki rétt að vísað sé til varnarmálalaga og reglugerðar nr. 959/2012 í þessu samhengi. Enn fremur gerir ríkislögreglustjóri athugasemd við skilgreiningu hugtaksins “Top Secret” undir reitnum “Raunlægar öryggiskröfur og merkingar” en sú merking fellur undir fyrrgreint alþjóðlegt flokkunarkerfi. Því telur embættið ekki æskilegt að nota hugtök úr alþjóðlega flokkunarkerfinu á þessum vettvangi.

Þá bendir embættið einnig á að í skilgreiningunni segir “Merkt „TOP SECRET“ eða með öðrum afgerandi hætti á öllum miðlum”. Slíkt orðalag er opið fyrir túlkun eða vali notanda á hugtakinu og/eða merkingunni. Leiðbeiningar sem þessar, sem ætlað er að stuðla að samræmdu verklagi innan stjórnsýslunnar, þurfa að vera skýrar og afdráttarlausar með stöðlun hugtaka fremur en vali.

RÍKISLÖGREGLUSTJÓRI

Undir reitnum “Öryggiskröfur starfsfólks” segir „*Starfsfólk sem hefur hlotið sérstaka þjálfun, gengist undir viðeigandi bakgrunnsathuganir og ef við á fengið öryggisvottanir af viðeigandi aðila, t.d. Ríkislögreglustjóra*“. Embætti ríkislögreglustjóri vekur athygli á að hvergi annars staðar í leiðbeiningum þessum er gerð grein fyrir kröfum um bakgrunnsskoðanir og útgáfu öryggisvottana til handa starfsfólki. Við framkvæmd bakgrunnsskoðunar felst töluvert inngríp í líf þeirra einstaklinga sem bakgrunnsskoðun sæta. Því þurfa bæði heimildir til bakgrunnsskoðunar að vera fyrir hendi af hálfu löggjafans sem og skýr hæfisviðmið einstaklinga til að standast bakgrunnsskoðun. Af skilgreiningunni má ætla að annars vegar þurfi starfsfólk bakgrunnsskoðun til að meðhöndla gögn í flokknum „afmörkuð gögn“ og hins vegar öryggisvottun í einhverjum tilfellum eða *ef við á* líkt og stendur í skilgreiningunni. Er það mat embættis ríkislögreglustjóra að slíkt orðalag sé opið til túlkunar og of matskennt til að samrýmast verklagi um öryggisflokkun gagna íslenska ríkisins. Notendum gagnanna þarf að vera það ljóst og ekki má leika um það vafi hvort öryggisvottunar sé krafist við meðhöndlunina eða ekki.

Samantekt á helstu ábendingum embættis ríkislögreglustjóra

Ábendingar embættis ríkislögreglustjóra, í samræmi við ofangreinda umfjöllun, snúa einkum að því að brýnt sé að leggja áherslu á að öryggiskröfur þurfi að vera skýrar og afdráttarlausar. Flestar öryggiskröfur, eins og þær koma fram í skýrslunni, eru huglægar/matskenndar og orðalag opið til túlkunar. Einnig er talin þörf á að setja ramma í löggjöf með nánari útfærslu á lágmarksöryggiskröfum svo tryggja megi gagnsæi og samræmt verklag innan stjórnsýslunnar. Skilgreina þarf ábyrgðaraðila (t.d. öryggisfulltrúa) og eftirlitsaðila (t.d. öryggisstjórnvald) sem hafa það hlutverk að tryggja að öryggiskröfum og öryggisráðstöfunum sé framfylgt innan allra stofnana ríkisins. Að lokum er talið brýnt að koma því á framfæri að gera þurfi skýrari greinarmun á annars vegar gildissviði leiðbeininga þessa og hins vegar gildissviði varnarmálalaga nr. 34/2008 og reglugerðar nr. 959/2012 um vernd trúnaðarupplýsinga, öryggisvottanir og öryggisviðurkenningar á sviði öryggis- og varnarmála.

Hér fyrir ofan hefur verið leitast við að koma á framfæri mikilvægustu atriðunum sem talið er brýnt að koma á framfæri við innihald skýrslunnar og í því sambandi er embætti ríkislögreglustjóra tilbúið að veita frekari upplýsingar og skýringar og koma að frekari vinnu með ráðuneytinu vegna þessa.