Október 2022

Öryggisflokkun gagna íslenska ríkisins

Data Security Classification of the Icelandic government

Stjórnarráð Íslands
Fjármála- og efnahagsráðuneytið

Útgefandi:
Fjármála- og efnahagsráðuneytið

Október 2022

fjr@fjr.is

www.fjr.is

Umbrot og textavinnsla:
Fjármála- og efnahagsráðuneytið

Efnisyfirlit

Útgáfa	Dagsetning	Samantekt á breytingum
0.1	18.02.2022	Drög til umræðu: Fyrsta útgáfa
0.2	8.4.2022	Skerping á orðalagi og hugtökum
0.3	25.5.022	Viðbætur og breytingar á grundvelli vinnufunda í maí 2022.
0.4	20.6.2022	Útgáfa til birtingar í opnu samráðsferli í Samráðsgátt stjórnvalda
1.0	18.10.2022	Uppfærð útgáfa eftir umsagnir í Samráðsgátt stjórnvalda

Samantekt

Skjal þetta lýsir öryggisflokkun gagna í stjórnsýslu íslenska ríkisins:

- út frá öryggissjónarmiðum,
- í þágu skilvirkrar og samræmdrar hagnýtingar á gögnum og
- í samræmi við gildandi lög, reglugerðir og innlendar og alþjóðlegar skuldbindingar.

Öryggisflokkar gagna taka til allra gagna sem ríkisaðilar safna, vista, vinna með, búa til og gera aðgengileg, í þágu hlutverks síns, þ.m.t. gögn sem stafa frá eða gerð eru aðgengileg þriðja aðila.

Ríkisaðilar skulu styðjast við fjóra öryggisflokka:

- Opin gögn
- Varin gögn
- Sérvarin gögn
- Afmörkuð gögn

Hver flokkur kallar á tiltekna og viðeigandi öryggiseiginleika, byggt á mögulegum afleiðingum af gagnaleka, tapi, stillingu og virði gagnanna. Aukið öryggisstig gagna kallar á auknar varnir gegn utanaðkomandi vá. Að auki gætu upplýsingakerfi og þjónustur krafist sértækra varna til að stýra áhættu sem tengist heilleika og tiltækileika gagna. Hægt er að samræma ofangreinda öryggisflokka við eigin flokkunarkerfi eða notast við þá óbreytta.

1. Inngangur

Flokkun gagna í öryggisflokka er ein af lykilforsendum þess að hægt sé að ná markmiðum stjórnvalda um aukna hagnýtingu gagna. Öryggisflokkar segja til um hvers konar varnir og ráðstafanir þarf að viðhafa fyrir gögn í viðkomandi flokki. Engin samræmd flokkun hefur verið viðhöfð hingað til í íslenskri stjórnsýslu og hefur skortur á slíkri samræmingu í för með sér að ekki er heldur til samræmd sýn á til hvaða öryggisráðstafana þarf að grípa til að verja gögn ríkisins. Ósamræmið hefur í för með sér aukinn kostnað í ríkisrekstrinum á sama tíma og skilningur og sýn ríkisaðila á sömu eða sambærileg gögn getur verið ólík. Þannig gæti ein stofnun litið á tiltekið skilgreint mengi gagna sem viðkvæmt á meðan önnur stofnun litið á sama gagnasett sem minna viðkvæmt.

Samræming og sameiginleg sýn á gögn og öryggisstig þeirra er því þjóðþrifamál til að auka hagnýtingu gagna og vitund um hverju þarf að kosta til við varnir gegn utanaðkomandi vá eða gagnaleka. Mikilvægt er að allir opinberir aðilar, s.s. sveitarfélag, hafi þessar flokkun til hliðsjónar í eigin gagnameðhöndlun og séu meðvitaðir um hana og afleiðingar mismunandi flokka til að auðvelda samskipti og gagnaflutninga við ríkisaðila, s.s. ráðuneyti.

Öryggisflokkun gagna hefur enn fremur áhrif á hvar og hvernig gögn eru geymd, hvort og hvernig þau eru unnin, samnýtt og gerð aðgengileg. Ein birtingarmynd í þessu samhengi er notkun skýjaþjónusta fyrir vistun og vinnslu gagna ríkisins. Ættu skýjaþjónustur t.d. að vera yfir höfuð leyfilegar við vistun gagna og er hægt að treysta vistun eða vinnslu gagna í skýjaþjónustum utan íslenskrar lögsögu? Eru gögn öruggari á netþjónum í rekstrarumhverfi tiltekinnar stofnunar? Til hvers konar stýringar og varna er hægt að grípa í umhverfi skýjaþjónustu í samanburði við staðbundna netþjóna?

Öryggisflokkun gagna er því í senn mikilvægt og gagnlegt tól til að svara áleitnum spurningum sem hafa mikil áhrif á rekstrarumhverfi og öryggisráðstafanir ríkisaðila.

Fjármála- og efnahagsráðuneytið hefur verið falið leiðandi hlutverk á sviði upplýsingatækni og stafrænni umbreytingu hins opinbera, þar á meðal samþættingu og notkun gagna innan ríkisrekstrarins.

Vinnuhópi var falið að leggja drög að öryggisflokkun gagna í nóvember 2021, í honum sátu fulltrúar forsætisráðuneytis, fjármála- og efnahagsráðuneytis, heilbrigðisráðuneytis og dómsmálaráðuneytis. Að auki sat í hópnum fulltrúi frá einkafyrirtækinu GRID. Vinnuhópurinn kynnti vinnu sína fyrir ráðuneytum og mikilvægum stofnunum sem framleiða, vista, vinna með og birta gögn.

2. Tilgangur

Tilgangur öryggisflokkunar gagna er sá að gögn séu flokkuð kerfisbundið og meðhöndluð á samræmdan og öruggan hátt. Flokkun byggir á virði gagna sem ríkisaðilum er falið að búa til, varðveita eða vinna auk þess að tryggja viðeigandi öryggisstig þeirra byggt á mati á mögulegum afleiðingum öryggisbrests, áhættum og ógnum sem telja má líklegt að steðji að þeim. Að standa vörð um leynd, réttleika og tiltækileika gagna er nauðsynlegt í öllum ríkisrekstri:

- Leynd vísar til að gögn séu ekki aðgengileg óviðkomandi aðilum eða vinnslum.
- Réttleiki vísar til þess að gögnin séu rétt, heil, óbrengluð og að allar breytingar séu gerðar af viðeigandi aðilum.
- Tiltækileiki vísar til að gögn séu aðgengileg viðeigandi aðilum þegar þeirra er þörf.

Byggir þessi skilgreining á þremur meginstoðum upplýsingaöryggis eins og þær eru skilgreindar í alþjóðlegum staðli um stjórnkerfi upplýsingaöryggis (ISO 27001), sem margir ríkisaðilar hafa til hliðsjónar eða innleitt að fullu. Eiginleika gagna, svo sem að þau séu heil (e. completeness) og að þau séu staðfestanleg (e. verifiable) má líta á sem afleiðingu af þessum þremur meginstoðum. Mögulegt er að beina athygli sérstaklega að slíkum eiginleikum og rúmast það innan þessara skilgreininga.

3. Umfang

Skylda ríkisaðila til að verja og tryggja öryggi gagna í sinni vörslu tekur til allra gagna sem þeir búa til, varðveita eða þeim eru afhent, m.a. skjöl á pappír og hvers kyns rafræn gögn. Leiðbeiningar þessar taka til aðila sem teljast til stjórnsýslu ríkisins og eru afhendingarskyldir aðilar[1]. Hér falla m.a. undir ráðuneyti, nefndir og stofnanir. Jafnframt aðilar sem fengið hefur verið til þess vald með lögum eða á grundvelli laga að taka stjórnvaldsákvarðanir eða sinna opinberum verkefnum. Leiðbeiningarnar taka auk þess til annarra aðila ef þeim hefur verið falin varsla gagna sem heyra til stjórnsýslu ríkisins. 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. Öryggisflokkun er mikilvægt verkfæri til að ríkisaðilar geti varið gögn sín á skilvirkan og árangursríkan hátt. Öðrum aðilum sem eru í miklum samskiptum við ríkisaðila getur verið nauðsynlegt að kynna sér þessa flokkun og þekkja afleiðingar hennar.

Svo tryggt sé að gögn séu tilhlýðilega varin þarf að kortleggja allar tegundir upplýsinga, skjala og gagna[2], þ.m.t. eiginleika, innihald þeirra og flokkun. Slík kortlagning er studd af skjalavistunaráætlunum, vinnsluskrám og upplýsingum úr stjórnkerfum upplýsingaöryggis yfir upplýsingaeignir.

Þessi öryggisflokkun gefur ekki heildstæða leiðsögn um innleiðingu eða val allra þeirra öryggis- og varnarúrræða sem nauðsynleg eru. Slíkt er aðeins mögulegt að teknu tilliti til annarra viðeigandi laga og reglugerða auk áhættumats. Afleiðingar sem vísað er til í þessu skjali geta þó t.d. stutt við framkvæmd áhættumats og þar af leiðandi val á öryggisúrræðum með samræmdari hætti en áður.

[1] Skv. lögum um opinber skjalasöfn, 14. gr.

[2] Sjá nánar í skilgreiningu hugtaka. Öll þrjú hugtökin, upplýsingar, gögn og skjöl eru notuð jöfnum höndum í þessu skjali.

4. Viðmið

Við þróun og gerð öryggisflokkunar gagna er stuðst við eftirfarandi viðmið (e. principles) sem gefa notendum flokkunarinnar leiðsögn ef vafi er um rétta meðferð og flokkun.

- Öll gögn hafa virði fyrir stjórnvald, einstakling, lögaðila eða samfélagið í heild.
- Viðhafa þarf viðeigandi og gagnsæja meðferð og viðeigandi öryggisúrræði gagna byggt á virði þeirra og tilgangi.
- Gögn skulu vera opin og aðgengileg öllum nema hagsmunir stjórnvalda, lögaðila, einstaklinga, almennings eða alþjóðasamstarf krefjist annars.
- Aðgangsstýringar sem beitt er til að verja gögn skulu byggja á lágmörkun réttinda, þ.e. aðeins þau sem þurfa aðgang hafi hann.
- Allir sem meðhöndla gögn í vörslu ríkisaðila, starfsfólk, þriðju aðilar og þjónustuaðilar skulu hafa viðeigandi kunnáttu í vörslu, umsýslu og öryggi gagna.

5. Áherslur

Megináherslur lýsa nálgun og veita leiðsögn um útfærslu flokkunarkerfisins og notkun þess. Sé flokkun óljós eða ekki skýrt hvernig flokka eigi eða skipta gögnum niður til að ná viðeigandi nákvæmni í flokkun er hægt að styðjast við þessar áherslur.

5.1 Áhersla 1: Gögn skulu vera opin nema annað sé ákveðið

Opin gögn skapa verðmæti fyrir samfélagið og því þarf að tilgreina sérstaklega ástæður fyrir því að gera gögn ekki aðgengileg almenningi. Samnýting gagna byggir á því að gögn séu aðgengileg þeim sem þurfa og styður það við einskráningu gagna (e. once only principle) og að notkun upplýsinga miðist við að gögn séu flutt á milli stofnana en ekki einstaklingar sem sækja þurfa þjónustu. Opin gögn skulu vera aðgengileg bæði notendum og öðrum kerfum á tölvulæsilegu (e. machine readable) sniði. Þegar talað er um opin gögn í þessu skjali er átt við gögn sem eru aðgengileg og nothæf fyrir samfélagið.

5.2 Áhersla 2: Öryggi gagna sé tryggt á viðeigandi hátt

Tilgreina þarf þær ógnir og afleiðingar, hvort sem um er að ræða fjárhagslegar, heilsufarslegar, þjóðaröryggislegar, orðspors eða af öðrum þeim toga, sem ætla má að brestir í öryggi gagna geti haft fyrir einstaklinga, lögaðila, stjórnvöld eða samfélagið í heild. Taka þarf mið af kröfum um leynd, réttleika og tiltækileika gagnanna við flokkunina, auk sjónarmiða um persónuvernd og réttindi einstaklinga. Innleiða skal nægjanlegar og viðeigandi öryggisráðstafanir byggt á kerfisbundnu áhættumati sem byggir á öllum þessum þáttum. Rétt innleiddar öryggisráðstafanir skulu stuðla að því að réttar upplýsingar séu tiltækar þegar þeirra er þörf hjá viðeigandi aðilum, bæði til skemmri tíma (í notkun) og lengri tíma (til varðveislu).

5.3 Áhersla 3: Flokkun gagna skal vera kerfisbundin og samræmd

Gögn geta eingöngu tilheyrt einum öryggisflokki út frá virði gagnanna. Flokkun fer fram út frá skilgreindum þáttum og eiginleikum og sérstaklega þarf að huga að því að sömu gögn geti ekki uppfyllt skilyrði tveggja flokka. Sé óvissa um flokkun skal nota lægra öryggisstig nema mögulegt sé að rökstyðja hærra öryggisstig og skal það rökstutt með vísun í lög eða niðurstöður kerfisbundins áhættumats. Afmörkun gagna í einsleitar einingar er forsenda þess að hægt sé að flokka þær með samræmdum og kerfisbundnum hætti.

5.3.1 Á3.1: Flokkar séu eins fáir og mögulegt er

Of margir flokkar skapa óvissu og flækjustig við ákvörðun um í hvaða flokki gögn eigi að vera. Hver flokkur þarf að endurspegla mismunandi kröfur og gögn sem falla undir hvern flokk þurfa að vera skýrt skilgreind.

5.3.2 Á3.2: Flokkun sé nákvæm og í samræmi við aðstæður á hverjum tíma

Skilgreiningar flokka þurfa að styðja við kerfisbundna flokkun og, að því marki sem mögulegt er, einnig sjálfvirka flokkun gagna. Flokka skal nægjanlega afmarkað safn gagna eða notkun þeirra svo varnir séu skilvirkar og taki til viðeigandi ógna. Flokkun skal vera rétt og uppfærð á hverju tíma m.v. virði og notkun gagnanna sem getur kallað á endurmat á flokkun.

5.3.3 Á3.3: Flokkun byggi á virði gagna

Afleiðingar af óviðeigandi notkun gagna stýra öryggisflokkun. Huga þarf að virði gagnanna bæði fyrir ríkisaðila og fyrir þá ytri aðila sem myndu mögulega vilja komast yfir þau.

5.4 Áhersla 4: Afleiðingar flokkunar skulu vera skýrar og skilgreindar

Flokkun gagna á að vera skýr fyrir alla sem koma að vinnslu og meðferð gagnanna, hvað varðar heimila notkun, vistun og meðferð.

5.4.1 Á4.1: Ábyrgð sé skýrt skilgreind

Ábyrgð á gögnum skal vera skýr og tilgreindur ábyrgðaraðili ber ábyrgð á að setja skýr viðmið og kröfur um meðhöndlun gagna, þ.m.t. flokkun þeirra, að gögn séu uppfærð og þeim sé rétt lýst í lýsigögnum til að hámarka hagnýtingu þeirra.

5.4.2 Á4.2: Meðhöndlun gagna byggi á samræmdri flokkun

Mikilvægt er að viðmið um meðhöndlun út frá samræmdri flokkun séu skýr svo aðilar komist að sömu niðurstöðu um meðferð og notkun gagnanna. Þannig er öryggi viðhaldið á fullnægjandi og skilvirkan hátt og möguleikar til samnýtingar hámarkaðir.

6. Hlutverk og ábyrgð

6.1 Ábyrgðaraðili gagna

Forstöðumaður ríkisaðila ber ábyrgð á flokkun gagna, viðeigandi varðveislu og umsýslu þeirra. Forstöðumaður getur falið öðrum að bera ábyrgð á meðhöndlun gagna sem berast eða eru búin til innan stjórnvaldsins. Að öllu jöfnu ætti sá einstaklingur að vera stjórnandi hjá viðkomandi ríkisaðila. Eigi gögnin uppruna hjá einstaklingi skal líta til þess hvaða ríkisaðili er frumskráningaraðili gagnanna og telst sá aðili þá vera ábyrgðaraðili og ber honum að flokka og setja kröfur um meðhöndlun og varðveislu.

Athygli er vakin á því að skilgreiningar á ábyrgðaraðila í þessu samhengi þarf ekki að fara saman með skilgreiningu á ábyrgðaraðila í tengslum við lög um persónuvernd og vinnslu persónuupplýsinga nr. 90/2018.

Dæmi um gögn

Fyrirtækjaskrá er skrá sem Skatturinn safnar gögnum í, viðheldur og gerir aðgengilega. Skatturinn ber ábyrgð á að skráin sé rétt, hún sé aðeins aðgengileg í samræmi við lög og reglur og að upplýsingar séu fjarlægðar úr henni ef þarf. Ríkisskattstjóri getur falið sviðsstjóra innheimtu- og skráasviðs að vera ábyrgðaraðili þessara gagna.

Sjúkraskrár innihalda upplýsingar um einstaklinga, heilsu fólks, meðferðarúrræði og greiningar sjúkdóma. Ýmsar heilbrigðisstofnanir geta haldið sjúkraskrá byggt á leyfi frá Embætti landlæknis. Hver og ein heilbrigðisstofnun er ábyrg fyrir því safni sjúkraskráa sem hún býr til, móttekur, safnar, vinnur og miðlar. Forstjóri heilbrigðisstofnunar getur falið t.d. framkvæmdastjóra lækninga að vera ábyrgðaraðila sjúkraskrárupplýsinga stofnunarinnar. Einstakar sjúkraskrár einstaklinga geta þó verið í ákveðnum skilningi „eign“ viðkomandi einstaklings en það hefur ekki áhrif á umfang eða eðli ábyrgðar stofnunarinnar á varðveislu safns sjúkraskráa.

6.2 Vörsluaðili gagna

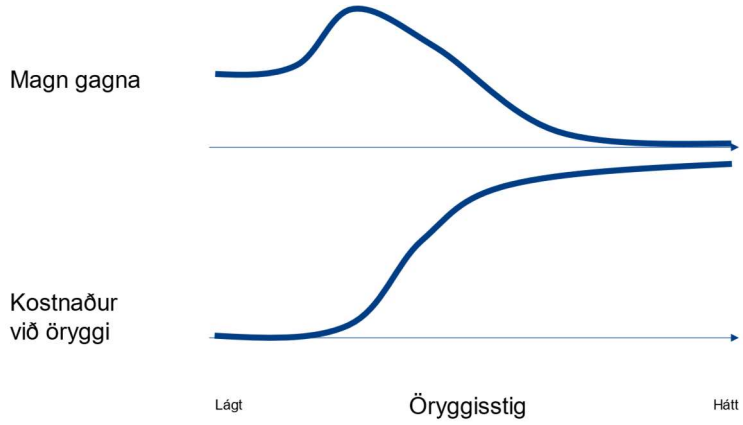
Ábyrgðaraðili gagna getur falið vörsluaðila eða tekið á sig þær skyldur sjálfur að sjá um daglega umsjón (vörslu) gagna, byggt á forsendum og forskrift. Vörsluaðili er sá aðili sem þarf að sjá til þess að fyrirmælum sé framfylgt og að viðeigandi öryggisúrræði séu innleidd í samræmi við ákvarðanir ábyrgðaraðila. Innri sem ytri þjónustuveitendur eða skýjaþjónustuveita geta séð um framkvæmd og rekstur öryggisúrræða en ábyrgðaraðili er ábyrgur fyrir að tryggja að lagalegar og viðskiptalegar kröfur séu uppfylltar í þeim öryggisúrræðum sem þriðji aðili starfrækir.

6.3 Notandi gagna

Notendur gagna bera aukna ábyrgð á flokkun, merkingu og stýringum á meðferð gagna frekar en að kerfi eða uppsetningar stjórni því. Notendur gagna geta verið starfsfólk viðkomandi stjórnvalds, annarra stjórnvalda, einstaklingar, félag eða lögaðili sem hefur aðgang að, notar eða uppfærir gögnin að staðaldri eða með reglubundnum hætti. Tilfallandi afhending eða notkun gagna út frá öðrum forsendum gera viðtakendur almennt ekki að notendum gagna. Notendur gagna bera ábyrgð á að framfylgja þeim reglum sem settar eru um meðhöndlun gagna. Kynna þarf og veita fræðslu til allra notenda gagna um þessar reglur. Með aukinni notkun almennra upplýsingakerfa sem veita notendum möguleika til að veita og stýra aðgangi að gögnum sjálfir og nota önnur öryggisúrræði, s.s. dulritun, eykst þörfin á að fræða og þjálfa notendur og veita notendum skýra leiðsögn um flokkun og meðhöndlun gagna. Í framhaldi af þessari flokkun verða slíkar leiðbeiningar unnar í samráði við hagsmunaaðila.

7. Öryggisflokkun gagna

Öryggisflokkun byggir á virði gagna og afleiðingum óviðkomandi aðgangs, misnotkunar, taps eða að gögnin séu röng. Flokka skal gögn með þeim hætti að viðeigandi öryggisstig náist, þ.e. að það verði hvorki of hátt né of lágt. Of hátt öryggisstig flokkunar getur valdið óþörfum kostnaði, flækjustigi í vinnulagi og kerfum og þannig hamlað nýtingu gagnanna.



Almenn skýring á umfangi gagna ríkisins og kostnaði vegna öryggisráðstafana

Dæmi um afmörkun

Tölvupósthólf ráðherra: Of víðtæk gagnaeining til að hægt sé að meta og því þarf að skipta upp í smærri flokka eftir innihaldi, þ.e.a.s. einstaka tölvupósta.

Dómsúrskurðir: Eru í mismunandi flokkum eftir því hvar í málsmeðferð gögnin eru. Geta orðið opnir þegar úrskurði er lokið og gerðir ópersónugreinanlegir.

Grunnskrár: Öryggisstig er mismunandi eftir því hvort verið er að varðveita, vinna eða miðla upplýsingum.

Vernd gagna skal miðast við að viðeigandi ráðstöfunum sé beitt á gögnin til að verjast ógnum og uppfylla lagalegar kröfur. Varnaraðgerðir umfram viðmið skulu vera byggðar á kerfisbundnu áhættumati. Þegar áhættur eru metnar skal litið til leyndar, réttleika og tiltækileika gagnanna auk þátta sem tengjast persónuvernd. Meta skal ógnir út frá virði gagna, þ.e. hversu mikið ætla má að ytri aðili myndi leggja á sig til að komast í gögnin í framkvæmd, kostnaði og orðsporsáhættu. Líta skal til þess hvaða aðilar gætu haft hag eða ávinning af því að komast yfir gögnin, hvort heldur það eru einstaklingar, fyrirtæki, aðilar með tengsl við skipulagða glæpastarfsemi eða erlend stjórnvöld. Meta þarf hver mögulegur ávinningur getur hlotist af af uppljóstrun eða spillingu gagnanna og gera ráð fyrir að viðkomandi aðilar, innri sem ytri, séu reiðbúnir til að verja fjármunum og fyrirhöfn í réttu hlutfalli við þann ávinning. Tryggja þarf að flokkun sé byggð á núverandi stöðu og aðstæðum og bestu fyrirliggjandi forsendum og staðreyndum hverju sinni. Tæknilegar lausnir er hægt að setja upp með þeim hætti að gögn innan þeirra uppfylli að jafnaði tiltekinn öryggisflokks. Hugbúnaðarkerfi geta auk þess gert mögulegt að verja sérstaklega ákveðin gögn (skjöl) í gagnasafninu og getur því innihaldið gögn sem eru í fleiri en einum öryggisflokki.

Meta skal áhættur út frá afleiðingum ógnar og notagildi gagnanna.

Hvenær skal meta viðkvæmnis- eða öryggisstig gagna?

Mat og flokkun skal framkvæma eins fljótt og mögulegt eftir að þau verða til þannig að hægt sé að verja þau með viðeigandi hætti frá upphafi.

Afmörkun upplýsinga, sem flokkaðar eru hverju sinni, skal vera eins nákvæm og einsleit og kostur er til að tryggja að hægt sé að flokka, meðhöndla og verja upplýsingarnar á viðeigandi og nægjanlegan hátt. Ef kröfur til verndar eru ekki samræmdar í öllu gagnasafninu/upplýsingunum þarf að skipta því upp til að hægt sé að flokka og meðhöndla á viðeigandi hátt. Endurskoða þarf þessa skiptingu reglulega til að tryggja að umfang sé viðeigandi á hverjum tíma. Miða skal við að hver afmörkun:

- Styðji við opna og gagnsæja stjórnsýslu
- Gerir ríkisaðila ábyrga fyrir ónægjanlegri flokkun eða flokkun í of hátt öryggisstig
- Auðveldar eftirlit með viðeigandi notkun gagna í rekstri ríkisaðila
- Stuðlar að aukinni skilvirkni og hagræðingu í gagnastýringu þvert á ríkisaðila

Mikilvægt er að taka upplýsta ákvörðun ef hækka á öryggisflokkun gagna. Sé óvissa um flokkun er mikilvægt að líta til sértækrar áhættu og úrræða fyrst áður en gögn eru flutt í hærri flokk. Flokkun gagna í of hátt öryggisstig getur leitt af sér að:

- Aðgengi að gögnum sé óþarflega takmarkað
- Stjórnunarleg og upplýsingatæknileg umsýsla verði óþarflega mikil, sem leiðir til hærri kostnaðar
- Öryggisflokkar séu ekki virtir eða hunsaðir af starfsfólki og viðtakendum gagnanna
- Of stór gagnasöfn í of háum öryggisflokki takmarkar hagnýtingu gagnanna, t.d. til að veita betri þjónustu, skapa aukin verðmæti eða taka betri ákvarðanir byggðum á gögnum
- Óvissa um flokkun og óskýr mörkun gagna leiðir oft til óþarflega hárrar flokkunar

Stofnandi skjals skal endurmeta flokkun þeirra gagna sem hann hefur öryggisflokkað, m.t.t. hækkunar, lækkunar eða afléttingu trúnaðar. Það skal gert reglulega í samræmi við viðmið um viðkomandi öryggisflokk. Ekki er heimilt að breyta öryggisflokkun eða aflétta trúnaði gagna í eigu annarra án þeirra samþykkis.

Er hætta á að öryggisflokkun gagna ýti undir flokkun gagna í hærri öryggisflokk og þar með áhættufælni ríkisaðila?

Ekki er búist við að ríkisaðilar flokki gögnin í hærri öryggisflokk á grundvelli öryggisflokkunar ríkisins. Þó er bent á að nálgun og áherslur flokkunarinnar eru sumpart ólík núverandi fyrirkomulagi. Þar má nefna talsvert aukna ábyrgð þeirra einstaklinga sem vinna með gögn og stuðning og hvatningu við notkunar staðlaðra hugbúnaðarlausna í stað sérsmíðaðra. Þessi áherslubreyting gæti þýtt að áhættusækni eða -fælni ríkisaðila getur breyst og að ríkisaðilar horfi fremur til aukinnar fræðslu og meðvitundar um notkun gagna í stað þess að áhersla þeirra sé fyrst og fremst á tæknilegar öryggislausnir eða högun.

7.1 Afmörkun til flokkunar

Þegar ákveðið er hvert umfang hvers gagnasafns/upplýsinga sem á að flokka skal vera er mikilvægt að hvert umfang sé afmarkað á skýran og nákvæman hátt. Gögnin sjálf skulu ráða þessari afmörkun en ekki tæknilegar útfærslur s.s. gagnagrunnar eða hugbúnaðarkerfi. Hugbúnaðarkerfi geta innihaldið margar gerðir upplýsinga sem þarf að verja og skilgreina með ólíkum hætti. Einnig geta sömu upplýsingar þurft mismunandi flokkun eftir notkun eða tilgangi notkunar. Tryggja þarf að þeir aðilar sem flokka gögn þekki innihald þeirra og notkun og haft sé samráð við viðeigandi aðila ef óvissa er um innihald gagnanna.

Gagnagrunnar, hugbúnaðarkerfi og aðrar gagna- og skjalageymslur, raunlægar sem stafrænar, geta innihaldið margar gerðir gagna. Útfæra þarf stýringar eins nákvæmlega og hægt er utan um hverja gagnaeiningu til að forðast óþarfar og íþyngjandi aðgerðir til að tryggja jafnvægi milli öryggis, notagildis og kostnaðar. Sama hugbúnaðarkerfi getur uppfyllt mismunandi öryggisstig þegar það er innleitt, t.d. með auknum öryggisstýringum.

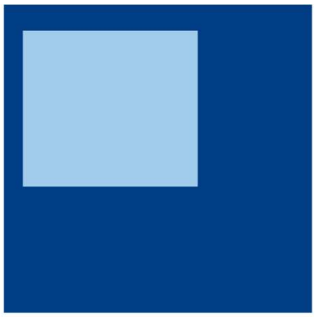
Of umfangsmikil skilgreining ákveðins gagnasafns getur leitt til þess að flokkun verði ónákvæm eða ómöguleg. Við slíkar aðstæður er mikilvægt að stjórnvöld endurskoði skilgreiningu flokkunar út frá t.d. ólíkum notkunarforsendum gagna og hvert notkunartilfelli (virði, eðli, innihald, umfang) sé skoðað. Það að gögn séu varðveitt í sama rekstrarumhverfi eða upplýsingakerfi gerir það ekki nauðsynlegt að öll gögn innan kerfisins tilheyri einu gagnasetti og séu flokkuð eins.

Taka þarf tillit til umfangs gagnasafns þegar afleiðingar uppljóstrunar, taps og rangra upplýsinga eru metnar. Dæmi um slíkt er fjöldi einstaklinga sem skráðir eru í gagnasafnið, samansafn upplýsinga frá mörgum lögaðilum um t.d. öryggisviðbúnað, samansafn upplýsinga um marga mikilvæga og viðkvæma staði sem einir og sér myndu ekki hafa miklar afleiðingar ef gögnum yrði uppljóstrað en ef öllu gagnasafninu yrði það væru umfangsmeiri afleiðingar.

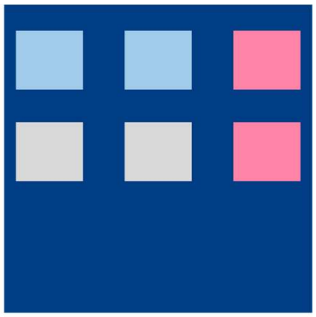
Að greina gögn niður í litlar, afmarkaðar einingar og taka tillit til þess að flokkun geti breyst á ákveðnum tímum gerir ríkisaðilum mögulegt að skiptast á skilvirkan og öruggan hátt á gögnum sem styður við opna og gagnsæja

stjórnsýslu. Sýnileiki, rekjanleiki og ábyrgð verða skýr fyrir hvert gagnasett og stýringar verða skilvirkari og árangursríkari.

Ef öll gögn eru í sama rekstrarumhverfi og varin með sama hætti er líklegt að einhver gögn séu ofvarin en önnur ekki varin nægjanlega vel



Með því að aðgreina ákveðin gögn eða vinnslur er hægt að hækka öryggisstig innan sama rekstrarumhverfis



Með því að aðgreina gögn og vinnslur eftir mikilvægi og öryggisstigi og sækja þjónustur frá mismunandi rekstrarumhverfum (staðbundið, hýst hjá þjónustuaðila eða skýjaþjónustu) er hægt að hámarka öryggisstig út frá eðli gagnanna

7.2 Skilgreiningar flokka

Ábyrgðaraðili skal flokka þær upplýsingar, skjöl og gögn sem hann ber ábyrgð á og leitast við að finna þann flokk þar sem viðeigandi öryggisstigi er náð. Sé ekki hægt að finna viðeigandi flokk skal kanna hvort hægt sé að greina gögnin í sundur út frá eiginleikum, notkun eða virði gagnanna. [3]

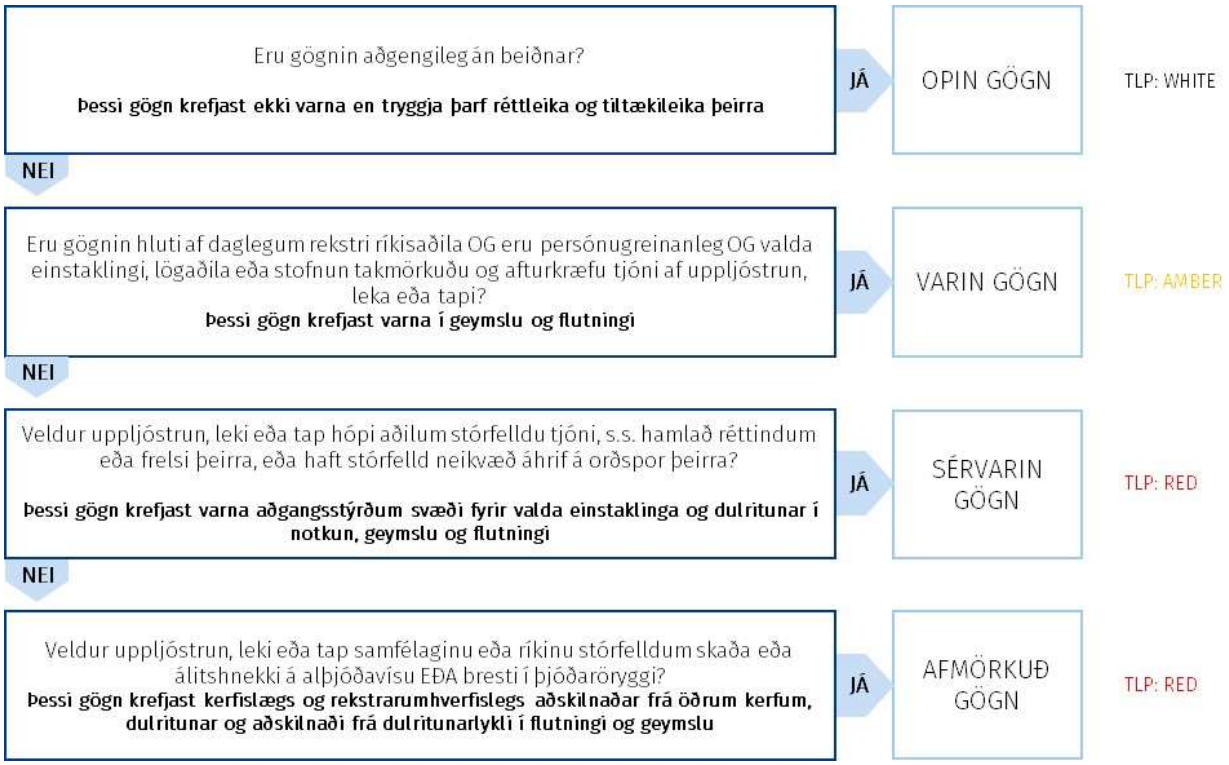
Í þessum kafla er leitast við að skilgreina eiginleika hvers flokks og afleiðingar fyrir gögnin sjálf. Fyrst er almennt fjallað um flokkana og svo settar fram nákvæmari lýsingar á eiginleikum flokkana og svo þeim viðmiðum um öryggisúrræði sem skal fylgja.

Í þessu skjali er notast við fjóra flokka gagna, sem öllum ríkisaðilum er leiðbeint að fara eftir og nýta í sinni starfsemi. Horft er til þess að flokkunin verði skyldubundin þegar reglur um meðferð trúnaðarupplýsinga verða settar. Gögn skulu flokkuð eftir því öryggisstigi sem virði þeirra gerir kröfu um:

1 - Opin gögn	Ópersónugreinanleg gögn eða gögn sem eru opin og aðgengileg til notkunar og endurnotkunar. Svo gögn teljist opin þurfa þau að vera tiltæk án umsókna / beiðna og vera aðgengileg óháð tíma.
2 - Varin gögn	Öll gögn önnur en opin gögn sem eru hluti af daglegum rekstri ríkisaðila. Varin gögn geta þó verið misviðkvæm og krafist sérsniðinna öryggisúrræða í samræmi við niðurstöður áhættumats.
3 - Sérvarin gögn	Gögn sem vegna viðkvæmrar stöðu m.t.t. tímasetninga eða innihalds geta valdið víðtæku og langvarandi tjóni fyrir hópa einstaklinga, lögaðila eða ríkisaðila.
4 - Afmörkuð gögn	Gögn sem eru viðkvæm fyrir samfélagið í heild eða stöðu þjóðarinnar á alþjóðavettvangi.

Til nánari skýringar á skilgreiningum flokka má styðjast við eftirfarandi ákvörðunartré / töflu:

[3] Dæmi um ólíka notkun sem getur kallað á mismunandi flokkun er varðveisla og miðlun grunnskrár eða þegar gögn eru tekin saman úr öðru gagnasafni og afhent á grundvelli t.d. upplýsingalaga[3]



	Opin	Varin	Sérvarin	Afmörkuð
Persónuvernd:				
Persónugreinanleg gögn (PII)	Nei	Já	Já	Já
Afleiðingar uppljóstrunar:				
Einstaklingur, lögaðili eða stofnun verður fyrir tjóni af uppljóstrun	Nei	Já	Já	Já
Veldur aðila tjóni sem hægt er að lágmarka eða afturkalla	Nei	Já		
Veldur aðilum stórfelldu tjóni, s.s hamlað réttindum eða frelsi þeirra	Nei	Nei	Já	Nei
Veldur samfélaginu stórfelldum skaða (einstaklingum/eignum)	Nei	Nei	Nei	Já
Veldur alþjóðlegum deilum	Nei	Nei	Nei	Já
Veldur álitshnekki ríkisins á alþjóðavísu	Nei	Nei	Nei	Já
Veldur bresti í þjóðaröryggi	Nei	Nei	Nei	Já

Sjá nánar í kafla 8 um „afleiðingar uppljóstrunar“ til frekari skýringar á hvaða öryggisflokk gögn tilheyra.

Taka skal fram að núverandi aðgangur eða aðgangsstýringar eru ekki endilega forskrift að því í hvaða öryggisflokk gögn muni lenda samkvæmt þessari flokkun.

7.3 Vistunarstaðir gagna

Ein mikilvægasta spurningin sem öryggisflokkun er ætlað að veita leiðsögn um er hvar heimilt sé að vista gögn. Mikilvægt er að horfa heildstætt til flokkunar, hugbúnaðarkerfa, vistunarstaðar og öryggisúrræða. Eftirfarandi tafla gefur þessi viðmið á samanteknu formi:

Flokkur	Staðsetning vistunar	Öryggisúrræði (viðmið)
Opin gögn	Hjá hæfum aðila innan EES sem uppfyllir öryggiskröfur og er t.d. aðili að innkaupaferli Ríkiskaupa. Ríkisaðili getur talist hæfur að uppfylltum öryggiskröfum.	Tryggja réttleika og tiltækileika.
Varin gögn	Hjá hæfum aðila innan EES sem uppfyllir öryggiskröfur og er t.d. aðili að innkaupaferli Ríkiskaupa. Ríkisaðili getur talist hæfur að uppfylltum öryggiskröfum.	Dulritun í flutningi yfir óörugg net og varið í geymslu fyrir óviðkomandi aðgangi. Auðkenning hvers notenda og allra aðgerða. Atburðaskráning uppflettinga og aðgangstilrauna.
Sérvarin gögn	Hjá hæfum aðila innan EES sem uppfyllir öryggiskröfur og er t.d. aðili að innkaupaferli Ríkiskaupa. Ríkisaðili getur talist hæfur að uppfylltum öryggiskröfum. Sértæk lög og kröfur geta takmarkað vistunarstaði.	Dulritun (með eigin lykli eða aðferðum) í notkun, flutningi og geymslu. Sterk og margþátta auðkenning, atburðaskráning uppflettinga og aðgangstilrauna. Sérhönnuð upplýsingakerfi byggð á sértækum öryggis- og virknikröfum miðað við eðli og virði gagnanna.
Afmörkuð gögn	Á sértækum og aðskildum upplýsingakerfum í eigu viðkomandi ríkisaðila.	Allt ofangreint auk aðskilnaðar frá öðrum kerfum.

Mat á hæfni vinnslu- og vistunaraðila gagna óháð staðsetningu innan EES þarf að fara fram, þ.m.t. birgjaúttektir sem taka til persónuverndar og vinnslu persónuupplýsinga. Hæfi aðila getur einnig verið innbyggt í opinbert innkaupaferli. Ábyrgðaraðili skal meta hæfni og getu aðila til að uppfylla kröfur varðandi öryggisúrræði, vernd og aðgengi gagna, þol við áföllum og öðrum innri sem ytri ógnum sem eiga við hverju sinni. Ríkisaðili er ábyrgur fyrir því að velja aðeins þá hýsingaraðila og staði sem uppfylla viðeigandi öryggiskröfur. Öryggisflokkun, innkaupaferli, áhættugreiningar og birgjarýni eru verkfæri sem styðja við það val. Huga þarf að öryggiskröfur til leyndar, réttleika og tiltækileika hjá vistunaraðilum og einnig ef ríkisaðili vistar gögnin sjálfur t.d. að tryggja aðgangsstýringar og afritun gagna sem geymd eru á miðlægum þjónum eða jafnvel borð- og fartölvum starfsfólks.

Ríkisaðilar geta leitað ráðlegginga og ráðgjafar hjá ýmsum aðilum, þ.m.t. á sviði upplýsingatækni, öryggismála og innkaupa til leiðbeininga um flokkun og meðhöndlun gagna. Miðlæg ráðgjöf á þessu sviði er hluti af aðgerðaáætlun og eftirfylgni þessa skjals. Endanlega ábyrgð á flokkun er þó alltaf hjá ábyrgðaraðila gagnanna.

8. Viðmið um meðhöndlun og öryggisúrræði

Eftirfarandi tafla tekur á ýmsum þáttum í meðferð gagna, aðgerðum til að verja trúnað, réttleika og tiltækileika auk varðveislu og mismunandi meðhöndlunar s.s. rafrænna gagna, á pappír eða öðru geymsluformi. Þau viðmið sem sett eru fram fyrir hvern flokk eru til viðmiðunar, hægt er að ná fram tilteknu öryggisstigi með öðrum aðgerðum sem gefa sambærilegar niðurstöður. Auk þess er ábyrgðaraðila heimilt að setja sértæk skilyrði eða úrræði fyrir varin, sérvarin eða afmörkuð gögn byggt á t.d. áhættumati. Viðmið hvers flokks eru til viðbótar við kröfur lægri flokka nema kröfur séu ósamrýmanlegar, þá gilda hærri kröfur.

Flokkur	Opin	Varin	Sérvarin	Afmörkuð
Skilgreining	Ópersónugreinanleg gögn eða gögn sem eru opin til notkunar og endurnotkunar. Svo gögn teljist opin þurfa þau að vera tiltæk án umsókna / beiðna og vera aðgengileg óháð tíma.	Öll gögn önnur en opin gögn sem eru hluti af daglegum rekstri ríkisaðila	Gögn sem vegna tímasetninga eða innihalds sem geta valdið víðtæku og langvarandi tjóni fyrir hópa einstaklinga, lögaðila eða ríkisaðila.	Gögn sem eru viðkvæm fyrir samfélagið í heild eða stöðu þjóðarinnar á alþjóðavettvangi.
Afleiðing upplýstrunar	Upplýstrun hefur engin áhrif en villur/spilling gagna getur valdið óþægindum eða rangri ákvarðanatöku stjórnvalda eða annarra.	Upplýstrun veldur stofnun eða tilteknum einstaklingi eða lögaðila óþægindum eða takmörkuðu fjárhagslegu eða orðsporstjóni sem mögulegt er að lágmarka. Upplýstrun getur valdið stofnun eða öðrum aðila óhagræði í samningum eða viðræðum við ytri aðila. Upplýstrun varðar við lög, t.d. brots á persónuvernd og kafla XIV í lögum nr. 19/1940.	Upplýstrun gæti valdið samfélagshópum (einstaklingar og lögaðilar) eða stjórnvöldum fjárhagslegum eða óefnislegum verulegum skaða og haft áhrif á líf, frelsi eða réttindi einstaklinga. Upplýstrun getur stöðvað alla starfsemi viðkomandi stofnunar eða mikilvægra innviða. Upplýstrun hefur marktæk áhrif á fjármálastöðugleika.	Upplýstrun stefnir öryggi og frelsi stórra samfélagshópa í verulega hættu. Upplýstrun skaðar samskipti við vinveittar þjóðir. Upplýstrun varðar við lög um varnarmál (nr. 34/2008) þ.m.t. sektum eða fangelsi í allt að fimm ár.
Afleiðing taps / einskis tiltækileika	Lágmarksáhrif á ríkisaðila, gögn er hægt að endurskapa út frá öðrum gögnum án mikillar fyrirhafnar. Ytri aðilar sem nýta gögn geta orðið fyrir óverulegu tjóni.	Ótiltækar upplýsingar geta valdið ríkisaðila óhagræði, einstaklingi eða öðrum lögaðila töfum eða tjóni sem þó er hægt að leiðrétta án þess að það hafi áhrif á rekstur ríkisaðila á verulegan hátt eða langvarandi áhrif á líf viðkomandi einstaklings.	Ótiltækar upplýsingar geta valdið einstaklingum eða hópum í samfélaginu verulegu tjóni sem erfitt er að leiðrétta t.d. að missa réttindi eða frelsi. Tapist upplýsingar er það mjög kostnaðarsamt eða ómögulegt fyrir ríkisaðila að endurskapa upplýsingarnar.	Afleiðingar taps eru sambærilegar við sérvarin.
Afleiðing rangra uppl.	Ríkisaðili verður fyrir lítillegum álitshnekki en upplýsingar er auðveldlega hægt að leiðrétta og tilkynna notendum um uppfærðar upplýsingar.	Rangar upplýsingar geta valdið tjóni fyrir einstakling, mögulegu afmörkuðu tjóni fyrir ríkisaðila sem mögulegt er að leiðrétta sem hluta af daglegum störfum og skyldum.	Rangar upplýsingar geta valdið hópum einstaklinga eða ríkisaðila tjóni sem erfitt eða mjög kostnaðarsamt er að bæta. Fjárhagslegt tjón umfram getu eins ríkisaðila til að bæta.	Rangar upplýsingar gætu valdið alþjóðlegum deilum eða skaðað samskipti við vinveittar þjóðir.

Flokkur	Opin	Varin	Sérvarin	Afmörkuð
Ábyrgð ríkisaðila	Að gögn séu uppfærð og rétt í samræmi við útgefin lýsigögn. Að lýsigögn séu uppfærð og rétt m.v. gögnin og að þau séu á tölvulesanlegu formi.	Tilgreindur hópur innan stofnunar eða milli stofnana hefur aðgang (e. need-to-know). Ytri aðili með lögmætan aðgang eða heimild getur haft hann.	Tiltekinn aðili ber ábyrgð á skilgreiningu aðgangs og meðferðar.	Tiltekinn einstaklingur í krafti embættis síns eða alþjóðlegs samstarfs.
Stýringar	Útgáfustýringar, sjálfvirkar uppfærslur og afhendingaröryggi sé metið, skjalfest og framfylgt. Flokkun er ekki endurskoðuð nema innihald breytist.	Aðgangsstýringar: Hópar Varin í flutningi yfir örugg samskiptakerfi með dulritun eða öðrum sambærilegum hætti. Varðveitt á aðgangsstýrðum svæðum og varin fyrir óviðkomandi aðgangi með viðeigandi hætti, þ.m.t. dulritun eða öðrum úrræðum. Flokkun er endurskoðuð reglubundið eða við ákveðin skilyrði í vinnslu.	Aðgangsstýringar: Tilgreindir einstaklingar með sérstakri heimild ábyrgðaraðila. Flokkun getur verið mismunandi á mismunandi tímum eða stöðu gagna (útgefið, drög, o.s.frv.). Afleidd, samantekin eða breytt gögn geta fallið í aðra flokka t.d. birting í mismunandi tilgangi.	Aðgangsstýringar: Kerfislægur aðskilnaður undirliggjandi upplýsingatækniumhverfa. Dulritað í flutningi og varðveislu og dulritunarlykill varðveittur í aðskildu umhverfi (t.d. HSM). Afritum af gögnum skal eytt á viðurkenndan hátt í samræmi við öryggisstig þegar þeirra er ekki þörf og þegar þeirra er ekki þörf vegna lagaskyldu.
Meðhöndlun (þ.m.t TLP / Traffic Light Protocol) [4]	Tryggt að gögn séu uppfærð og rétt á geymslustöðum sem eru tiltækir eftir þörfum. Vistað á viðeigandi hátt innan EES. TLP:WHITE	Aðgengileg þeim hópum sem hafa lögmæt rök fyrir aðgangi (t.d. á grundvelli verkefna, starfs) innan sama ríkisaðila eða hjá öðrum ríkisaðila sem vegna lögbundinnar þjónustu þarf aðgang. Þarf að meta sérstaklega kröfur um varðveislu (skil). Áhættumat framkvæmt út frá virði gagnanna. Vistað á aðgangsstýrðum gagnageymslum/svæðum innan EES. TLP:AMBER	Afhendist aðeins tilgreindum einstaklingum. Krefst sértæks áhættumat á allri vistun og notkun gagna, sem gæti t.d. kallað á sértæk öryggisúrræði. Upplýsingakerfi skulu vera innan EES hjá vottuðum aðilum og með óskiptum yfirráðum ábyrgðaraðila gagnanna. TLP:RED	Aðeins unnið í aðgreindum kerfum sem hafa sérstaklega verið tekin út m.t.t. öryggisstigs. Búnaður og allt burðarlag í eigu viðkomandi stofnunar sem ber ábyrgð á gögnunum. TLP:RED

[4] Skýringar á TLP flokkun er að finna á vef CERT-IS: https://www.cert.is/um-cert-is/tlp/.

Flokkur	Opin	Varin	Sérvarin	Afmörkuð
Raunlægar öryggiskröfur og merkingar	Merkt uppruna og útgáfu (t.d. dagsetning). Lýsigögn til staðar.	Merkt tilteknu máli/verkefni sem gefur upplýsingar um hver skuli hafa aðgang. Gera óviljandi uppljóstrun ólíklega. Geymslustaðir og rými þar sem upplýsingakerfi sem hýsa gögn í þessum flokki skal verja með viðeigandi hætti fyrir raunlægum ógnum, s.s. aðgangi, eldi og náttúruhamförum að teknu tilliti til trúnaðar, réttleika og tiltækileika.	Sérstaklega tilgreint hver hefur aðgang og á hvaða grundvelli aðgangur er veittur.	Sérstaklega tilgreint hver hefur aðgang. Gögn skulu lokuð í dreifingu og flutningi. Merkt með afgerandi hætti óháð miðlum. Afhending skal aðeins vera með skjalfestum og viðurkenndum aðferðum sem tryggir að viðkomandi sé réttur aðili og að hann hafi tekið við sendingunni.
Rafrænar öryggiskröfur	Aðgengileg og opin skil á gögnum. Uppfærð og rétt skilgreind gögn á hverjum tíma.	Aðgangsstýringar byggðar á lágmörkun aðgangs. Vel varin fyrir sjálfvirkum eða tækifæris árásum á upplýsingakerfi. Upplýsingakerfi og hugbúnaður skulu vera innan EES með yfirráðum með samningnum eða öðrum hætti hjá ábyrgðaraðila/vörsluaðila. Fjölþáttaauðkenning byggð á áhættumati og hvernig aðgangur að gögnum og hugbúnaðarkerfi er háttað.	Aðgangur er takmaður og stýrður, ryndur og uppflettingar sem og tilraunir til að nálgast gögn skráð í hugbúnaðarkerfum. Kerfi og gögn eru vel varin fyrir árásum sem beinast sérstaklega að þeim og geta varist þeim. Auðkenning sem uppfyllir skilyrði um hátt auðkenningarstig (eIDAS) og LoA4 samkv. ISO29115. Tryggja hreinsun á óþörfum eintökum gagna. Aðgangur og uppflettingar skráðar niður á einstaklinga. Sérstök dulritun (own key), dulritað í öllum flutningi og geymslu.	Upplýsingakerfi og hugbúnaður eru sérskrifuð út frá sértækum öryggis- og virknikröfum og aðskilin með kerfislægum hætti svo mjög ólíklegt er að árás sem gerð er á þeim heppnist, t.d. með aðskilnaði endabúnaðar, netlags eða öðrum aðferðum. Allar aðgerðir, tilraunir til aðgangs og þær sem heppnast eru skráðar og ryndar reglulega af viðeigandi aðilum. Upplýsingakerfi skulu vera á fullri ábyrgð ábyrgðaraðila gagnanna, þ.m.t. undirliggjandi einingar s.s. vélbúnaður, net og raunlægur aðbúnaður.
Varðveisla	Tryggja þarf að varðveisla gagna t.d. ef opin gögn eru afleidd af öðrum gögnum sé viðeigandi. Hreinsun eldri útgáfa gæti verið nauðsynleg til að fyrirbyggja að rangar eða úreltar upplýsingar séu aðgengilegar.	Tryggja þarf að gögn séu skráð í skjalavistunaráætlanir ríkisaðila og að varðveisla þeirra sé tryggð bæði á rafrænu og raunlægu formi.	Tryggja þarf að gögn séu skráð í skjalavistunaráætlanir ríkisaðila og að varðveisla þeirra sé tryggð bæði á rafrænu og raunlægu formi. Huga þarf sérstaklega að hreinsun óþarfra eintaka til að lágmarka líkur á uppljóstrun eða röngum/úreltum upplýsingum.	Leita skal sérstaklega eftir ráðgjöf Þjóðskjalasafns um skráningu og skil gagna í þessum flokki. Opinbert skjalasafn getur í samráði við afhendingaraðila ákveðið að skjal verði fyrst aðgengilegt er liðin eru allt að 40 ár ef nauðsynlegt þykir til að vernda almannahagsmuni, sbr. 1. mgr. 28. gr. laga um opinber skjalasöfn.

Flokkur	Opin	Varin	Sérvarin	Afmörkuð
Öryggiskröfur starfsfólks	Birtar af aðilum sem þekkja til gagnanna og geta metið réttleika þeirra.	Starfsfólks er þjálfað og meðvitað um meðferð og öryggi gagna. Verktakar sem eru samningsbundnir (með trúnaðarákvæði).	Starfsfólk sem hefur fengið sértæka þjálfun í meðferð og öryggi viðkomandi gagna. Verktakar sem hafa undirritað sérstakar trúnaðaryfirlýsingar (einstaklingar) og fengið leiðsögn um meðhöndlun gagna.	Starfsfólk sem hefur hlotið sérstaka þjálfun, gengist undir viðeigandi bakgrunnsathuganir og þar sem við á fengið öryggisvottanir hjá viðeigandi aðila (Ríkislögreglustjóra) ef það á við. Verktakar sem hafa undirgengist sambærileg skilyrði.
Endurmat flokkunar	Aðeins ef innihald gagna breytist.	Endurmeta skal flokkun á a.m.k. fimm ára fresti eða ef innihald gagna breytist.	Endurmeta skal flokkun á a.m.k. fimm ára fresti, setja skal fram tímasettar breytingar t.d. um lækkun flokkunar.	Endurmeta skal flokkun á a.m.k. fimm ára fresti, setja skal fram tímasettar breytingar t.d. um lækkun flokkunar (sbr. reglugerð nr. 959/2012).

8.1 Afleiðingar af uppljóstrun, tapi og röngum upplýsingum

Í meðfylgjandi töflu er skilgreint nánar hver viðmið um afleiðingar fyrir mismunandi hópa/aðila eru fyrir gagnaflokkana.

Aðili	Afleiðing	Opin	Varin	Sérvarin	Afmörkuð
Einstaklingur	Uppljóstrun	Engin áhrif	Óþægindi eða takmarkað tjón sem auðvelt er að bæta.	Veruleg áhrif sem gætu hamlað réttindum eða frelsi einstaklings til lengri tíma.	Stefnir öryggi einstaklinga (oft fleiri en eins) í verulega hættu, þ.m.t. lífshættu.
Einstaklingur	Tap/Ekki tiltæk	Mjög lítil	Tafir, óþægindi eða takmarkað tjón sem auðvelt er að bæta.	Fjárhagslegt tjón eða takmörkun á réttindi eða frelsi sem gæti haft langvarandi áhrif í för með sér.	Sambærilegar afleiðingar og í sérvarin.
Einstaklingur	Rangar upplýsingar	Mjög lítil	Óþægindi eða takmarkað tjón sem auðvelt er að bæta.	Skerðing á réttindum eða frelsi sem er utan valdssviðs þess ríkisaðila að bæta.	Sambærilegar afleiðingar og í sérvarin.
Lögaðili	Uppljóstrun	Engin áhrif	Óþægindi eða takmarkað tjón sem auðvelt er að bæta.	Veruleg áhrif fyrir hagsmuni lögaðila, t.d. fjárhagslegt tjón sem þyrfti að sækja bætur fyrir með dómsmáli.	Sambærilegar afleiðingar og í sérvarin.
Lögaðili	Tap/Ekki tiltæk	Mjög lítil	Tafir, óþægindi eða takmarkað tjón sem auðvelt er að bæta.	Veruleg áhrif á fjárhag eða orðspor sem gætu dregið úr rekstrarhæfi lögaðila til lengri tíma.	Sambærilegar afleiðingar og í sérvarin.
Lögaðili	Rangar upplýsingar	Mögulega leitt til rangrar ákvarðanatöku í afmörkuðum málum.	Óþægindi eða takmarkað tjón sem auðvelt er að bæta.	Veruleg áhrif á fjárhag eða orðspor sem gætu dregið úr rekstrarhæfi lögaðila til lengri tíma.	Sambærilegar afleiðingar og í sérvarin.
Hópur	Uppljóstrun	Engin áhrif	Mjög lítil	Getur valdið tjóni fyrir hópa einstaklinga og lögaðila, t.d. fjárhagstjóni eða óefnislegum skaða.	Getur valdið alvarlegum varanlegum afleiðingum fyrir hópa, þ.m.t. dauða.
Hópur	Tap/Ekki tiltæk	Mjög lítil	Mjög lítil	Hópar einstaklinga gætu orðið fyrir orðspors eða efnislegum áhrifum sem takmarka réttindi og frelsi.	Sambærilegar afleiðingar og í sérvarin.
Hópur	Rangar upplýsingar	Mjög lítil	Mjög lítil	Hópar einstaklinga gætu orðið fyrir orðspors eða efnislegum áhrifum sem takmarka réttindi og frelsi.	Sambærilegar afleiðingar og í sérvarin.
Ríkisaðili	Uppljóstrun	Engin áhrif	Orðspors eða fjárhagsleg óþægindi sem mögulegt er að bæta.	Orðspors eða fjárhagslegt tjón sem krefst viðbragða umfram fjárheimildir eða hlutverk ríkisaðila.	Myndi gera ríkisaðila óhæfan til að starfrækja hlutverk sitt vegna orðsporsskaða. Uppljóstrun varðar við lög nr. 34/2008 um varnarmál.
Ríkisaðili	Tap/Ekki tiltæk	Mjög lítil	Tafir eða tjón sem hefur ekki veruleg áhrif á orðspor, fjárhag eða starfsemi ríkisaðila.	Tap gagnasafnsins í heild getur verið óafturkræft tjón sem ekki er hægt að bæta eða endurgera.	Sambærilegar afleiðingar og í sérvarin.
Ríkisaðili	Rangar upplýsingar	Mjög lítil	Tafir eða rangar ákvarðanir sem geta valdið orðspors áhættu, auknum kostnaði en hægt er að leiðrétta innan heimilda ríkisaðilans.	Tafir eða rangar ákvarðanir sem valda verulegri áhættu, kostnaði sem ríkisaðili getur ekki mætt innan fjárheimilda eða öðrum skaða.	Sambærilegar afleiðingar og í sérvarin.
Stjórnvöld	Uppljóstrun	Engin áhrif	Óveruleg fjárhagsleg áhrif fyrir stjórnvöld í heild, orðspors áhætta sem hefur ekki áhrif á stöðu landsins í alþjóðasamskiptum.	Áhrif sem gætu haft áhrif á hópa ríkisaðila (t.d. ákveðna geira) og krafist viðbragða af hálfu t.d. ríkisstjórnar til að bregðast við á fullnægjandi hátt.	Geta valdið alþjóðlegum deilum, skaðað samskipti við vinveittar þjóðir.
Stjórnvöld	Tap/Ekki tiltæk	Engin áhrif, gögn er hægt að endurgera út frá öðrum gögnum með auðveldum hætti.	Óveruleg fjárhagsleg áhrif fyrir stjórnvöld í heild, orðspors áhætta sem hefur ekki áhrif á stöðu landsins í alþjóðasamskiptum.	Skaði eða tafir á málefnum sem gætu valdið stjórnvöldum verulegu fjárhagslegu tjóni eða skaðað stöðu þeirra gagnvart samfélaginu.	Sambærilegar afleiðingar og í sérvarin.
Stjórnvöld	Rangar upplýsingar	Engin áhrif	Óveruleg fjárhagsleg áhrif fyrir stjórnvöld í heild, orðspors áhætta sem hefur ekki áhrif á stöðu landsins í alþjóðasamskiptum.	Getur kallað á viðbrögð að hálfu stjórnvalda til að leiðrétta eða upplýsa innlenda eða erlenda aðila.	Geta valdið alþjóðlegum deilum, skaðað samskipti við vinveittar þjóðir.

9. Tengsl við lög og aðrar kröfur

9.1 Lög um opinber skjalasöfn

Varðveisluskylda er á öllum skjölum og gögnum sem hafa orðið til, borist eða verið viðhaldið við starfsemi afhendingarskyldra aðila og er óheimilt að eyða nokkrum upplýsingum nema að heimild liggi fyrir samkvæmt lögum um opinber skjalasöfn.

Gagnaflokkun skal styðja við skjalavistunaráætlanir ríkisaðila og tryggja þarf að allir skjalaflokkar séu flokkaðir. Huga þarf sérstaklega að því að skjalaflokkar sem varða starfsemi ríkisaðila séu öll skráð í skjalavistunaráætlanir en gagnaflokkun getur verið nauðsynleg á önnur gögn sem ríkisaðili ber ábyrgð á, s.s. atburðaskrám upplýsingakerfa og öðrum slíkum gögnum.

Til að lágmarka áhættu vegna uppljóstrunar og rangra upplýsinga er mikilvægt að ríkisaðilar meti hvort að sækja þurfi sérstaklega um grisjunarheimildir ef gögn eru sérvarin eða afmörkuð. Sé slík heimild til staðar þarf að stafrækja sérstök úrræði eða verklagsreglur til að tryggja að skipulögð grisjun sé framkvæmd í samræmi við heimild.

Hreinsun gagna er nauðsynlegur hluti af frágangi og vinnslu í gagnasöfnum og skal hreinsa þau af öllum aukaeintökum, rissblöðum (drögum) eða sambærilegu. Með hækkandi öryggiskröfum er almennt nauðsynlegt að auka tíðni hreinsunar og skilgreina sérstaklega verklagsreglur eða tæknilegar útfærslur sem styðja við hreinsun,, t.d. með því að varðveita rafrænt undirrituð eintök aðeins á viðeigandi stöðum en hreinsa raunlæg afrit.

Ráðgjöf og leiðbeiningar Þjóðskjalasafns má finna á vefsíðu þess: https://radgjof.skjalasafn.is/

9.2 Lög um persónuvernd og vinnslu persónuupplýsinga

Gagnaflokkun skal styðja við að persónuupplýsingar séu unnar í samræmi við lög um persónuvernd og vinnslu persónuupplýsinga. Vinnslur sem m.a. eru skráðar í vinnsluskrár ríkisaðila geta tekið til eins eða fleiri gagna og mikilvægt að öll gögn sem innihalda persónuupplýsingar séu flokkaðar. Vinnsluskrá er þó ekki tæmandi listi yfir gagnasöfn sem ber að flokka því einnig ber að flokka gögn sem varða ekki tiltekna einstaklinga eða eru ópersónugreinanleg en geta haft virði og afleiðingar af uppljóstrun, tapi eða röngum upplýsingum getur verið til staðar.

Mikilvægt er að greina sérstaklega m.t.t. persónuupplýsinga hvort mikilvægi upplýsinganna fyrir skráða einstaklinga og réttindi þeirra, líf, frelsi og heilsu sé út frá afleiðingum taps (gögn ekki tiltæk til skemmri eða lengri tíma) eða vegna rangra upplýsinga eða uppljóstrun (óviðkomandi aðili komist yfir gögnin). Slík greining getur verið nauðsynleg til að flokka og útfæra öryggisúrræði í samræmi við þær sértæku áhættur sem steðja að einstaklingnum t.d. af umfangi vinnslunnar, vinnslubúnaði sem notaður er eða staðsetningu vinnslunnar. Persónugreinanleg gögn gæti þá verið skylt að birta með opinberum hætti.

9.3 Reglugerð um vernd trúnaðarupplýsinga (nr. 959/2012)

Reglugerð um vernd trúnaðarupplýsinga, öryggisvottanir og öryggisviðurkenningar á sviði öryggis- og varnarmála tekur sérstaklega til þeirra trúnaðarupplýsinga sem varnarmálalög, nr. 34/2008 taka til og aðgangs að trúnaðarupplýsingum á grundvelli samninga við Evrópusambandið, aðrar þjóðir og alþjóðlegar stofnanir.

Þær reglur og ákvæði sem gilda um gögn af því tagi ganga framar þeim viðmiðum sem sett eru fram í þessari öryggisflokkun. Huga þarf sérstaklega að afmörkun þeirra gagna sem reglugerðin á við og verja þau gögn í allri varðveislu og notkun í samræmi við reglugerðina. Einnig skal huga að aðgreiningu gagna í kerfum, hugbúnaði og annarri vinnslu svo að gögn sem falla ekki undir gildissvið reglugerðarinnar séu ekki meðhöndluð með sama hætti og þau sem falla undir hana eingöngu vegna þess að þau eru geymd í sömu kerfum/gagnageymslum. Mikilvægt öryggisatriði er að takmarka umfang hvers gagnasafns svo hægt sé að beita öryggisúrræðum með markvissum og skilvirkum hætti.

Gögn sem falla undir reglugerðina uppfylla að jafnaði skilyrði þess að flokkast sem afmörkuð (hæsti flokkur) og bætast þá kröfur reglugerðarinnar við þau viðmið og reglur sem gilda almennt um þann flokk í þessu skjali. Huga þarf sérstaklega að endurmati á öryggisflokkun og takmörkunum á aðgengi með reglubundnum hætti þegar um gögn er að ræða sem lenda í háum öryggisflokki.

9.4 Upplýsingalög

Gagnaflokkun styður við markmið upplýsingalaga um gagnsæi í stjórnsýslu, aðgengi að upplýsingum hins opinbera og að auka traust almennings á stjórnsýslu með því að beita kerfisbundnum aðferðum til að flokka og meðhöndla gögn hins opinbera.

Ríkisaðilar geta leitað sérstakrar ráðgjafar, ef þeir óska svo, vegna gagna í flokkunum sérvarin eða afmörkuð gögn á grundvelli upplýsingalaga. Flokkun gagnanna og rökstuðningur fyrir henni gæti gefið tilefni til takmarkana á grundvelli t.d. 9. eða 10. gr. upplýsingalaganna. Kerfisbundin flokkun byggð á gagnaflokkunarstefnu ætti að auka traust til stjórnvalda með að sýna fram á að ákvarðanir um takmarkanir séu teknar á grundvelli fyrirliggjandi flokkunar fyrir viðkomandi gagnasafn.

Afhent gögn á grundvelli upplýsingalaga geta t.d. verið hluti af heildargagnasafninu. Meðhöndla skal það gagnasafn sem sérstakt gagnasafn sem getur haft aðra flokkun en upprunalega gagnasafnið sem gögnin voru unnin úr.

9.5 Yfirlit laga og krafa sem algengt er að taka þurfi tillit til

- Lög um persónuvernd og vinnslu persónuupplýsinga nr. 90/2018.
- Upplýsingalög nr. 140/2012.
- Lög um endurnot opinberra upplýsinga nr. 45/2018.
- Lög um opinber skjalasöfn nr. 77/2014.
- Stjórnsýslulög nr. 37/1993.
- Varnarmálalög nr. 34/2008.
- Lög um öryggi net- og upplýsingakerfa mikilvægra innviða nr. 78/2019.
- Lög um réttindi og skyldur opinberra starfsmanna nr. 70/1996.
- Lög um lífsýnasöfn og söfn heilbrigðisupplýsinga nr. 110/2000.
    - 5. gr. skilyrði um staðsetningu hér á landi
- Lög um sjúkraskrár nr. 55/2009.
- Lög um vernd uppljóstrara nr. 40/2020.
- Fyrirhugað er að endurskoða lög um endurnot opinberra upplýsinga (Open Data Directive) m.t.t. tilskipunar Evrópuþingsins og ráðsins (ESB) 2019/1024 frá 20. júní 2019 um opin gögn og endurnotkun upplýsinga frá hinu opinbera. Flokkunin þarf að styðja við markmið þeirra.
- Fyrirhugað er að leggja fram lagafrumvarp um frjálst flæði ópersónugreinanlegra upplýsinga (Free Flow of Data) m.t.t. tilskipunar Evrópuþingsins og ráðsins (ESB) 2018/1807 frá 14. nóvember 2018. Flokkunin þarf að styðja við markmið þeirra.
- Ástæða kann að vera til að taka til skoðunar ákvæði ýmissa lagabálka sem varða sölu og notkun gagna stofnana, þ.m.t. til annarra stjórnvalda.

10. Næstu skref

Í kjölfar birtingar öryggisflokka gagna íslenska ríkisins verður unnið að því að útbúa nánari leiðbeiningar, handhæg verkfæri og greinarbetri upplýsingum fyrir ríkisaðila og birt á opnu vefsvæði ásamt öðru sem tengist stefnu um notkun rekstrar- og hýsingarumhverfis (skýjalausna), m.a.:

- Leiðbeiningar um almenna útfærslu á öryggisúrræðum til að bregðast við flokkun.
    - Leiðsögn um vistunaraðila og vernd upplýsinga m.v. staðsetningu.
    - Útfærslur á raunlægum öryggisúrræðum.
    - Útfærslur á rafrænum öryggisúrræðum.
- Viðmið um notkun og innkaup skýjalausna (tæknigrunnar skýjalausna)
- Áhættumatsgrunnur fyrir algengar og mikið notaðar skýjalausnir.
- Sniðmát og verkfæri til að styðja við kortlagningu og mat á flokkun gagna.
- Kynningar, fræðsla og upplýsingamiðlun bæði til stjórnenda, tæknilegra ábyrgðaraðila og almennt til starfsfólks um meðferð upplýsinga, hvað flokkun þýðir og hvaða afleiðingar þær hafa í daglegum störfum.

Íslenska ríkið hefur auk þess gefið út nokkrar stefnur sem jafnframt styðja við aukna hagnýtingu upplýsingatækni og gagna, sem gott að horfa til. Þar má nefna Öryggis- og þjónustustefnu um hýsingarumhverfi, Netöryggisstefnu Íslands og Stafræn stefna um opinbera þjónustu.

Hugtök

Hugtak	Skýring
Lýsigögn	Þær upplýsingar sem fylgja gögnum og segja frá innihaldinu, eðli, uppruna og vinnslu gagnanna. Gera notendum mögulegt að nota gögnin á réttan hátt og draga viðeigandi ályktanir af þeim. Lýsigögn skulu vera leitarhæf og gera bæði notendum og kerfum mögulegt að vinna gögn út frá innihaldi og eðli, þ.m.t. tengslum við lögaðila og einstaklinga, málaflokkum eða öðrum þáttum sem kunna að vera mikilvægir fyrir hvert og eitt gagnasett (*e. metadata*).
Tölvulesanlegt snið	Framsetning gagna með þeim hætti að kerfi/hugbúnaður geti með sjálfvirkum hætti (án aðkomu einstaklings) lesið, leitað og sótt gögnin í heild eða einstaka hluta þeirra t.d. með fyrirspurnum í vefþjónustur eða annan sambærilegan tæknilegan útbúnað (*e. machine readable*). Gögn skulu vera vinnslu- og leitarhæf, þ.e. bæði innihald og lýsigögn.
Þjóðaröryggi	Með þjóðaröryggi er átt við öryggi sbr. skilgreiningu í þjóðaröryggisstefnu fyrir Ísland.
TLP	Traffic Light Protocol – skilgreiningar frá FIRST. Sjá skýringar á íslensku hjá CERTÍS.
Ópersónugreinanleg gögn	Öll önnur gögn en persónugreinanleg gögn skv. skilgreiningu um persónuupplýsingar í lögum um persónuvernd 90/2018, sjá 2. tl, 1. mgr. 3. gr.
Ríkisaðilar	Aðilar sem fara með ríkisvald og þær stofnanir, sjóðir og fyrirtæki sem eru að hálfu eða meirihluta í eigu ríkisins, þó ekki stofnanir sem starfa á samkeppnismarkaði.
Upplýsingar	Upplýsingar á hvers kyns formi, þ. á m. stafrænu, rituðu, sjónrænu, heyranlegu og efnislegu.
Gagnasett	Eining sem rammar inn tiltekin gögn sem öll falla í sama flokk.
Skjöl og gögn	Hvers konar gögn, jafnt rituð sem í öðru formi, er hafa að geyma upplýsingar og hafa orðið til, borist eða verið viðhaldið, sbr. skilgreiningu í lögum um opinber skjalasöfn.
EES	Evrópska efnahagssvæðið, þ.e. aðildarríki Evrópusambandsins auk Íslands, Noregs og Liechtenstein.