

14. september 2022



Öryggisflokkun gagna ríkisins (Data Security Classification)

Hádegisfundur SKÝ

Stafræn stefna



Aukin samkeppnishæfni

Betri þjónusta

Öruggari innviðir

Nútímalegt starfsumhverfi

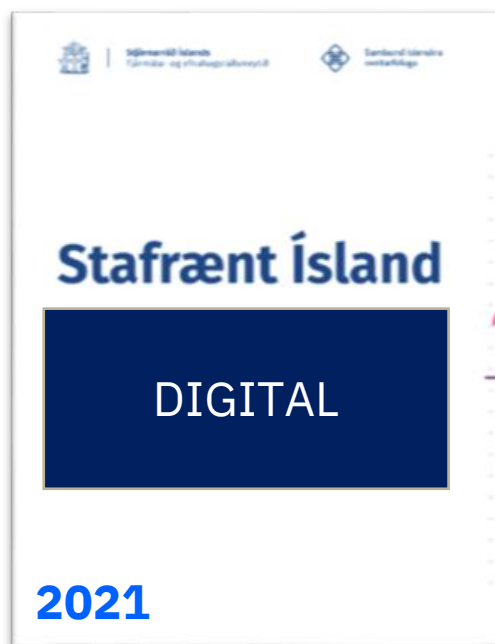
Skýjastefna



Aukið öryggi

Betri þjónusta

Meiri nýsköpun

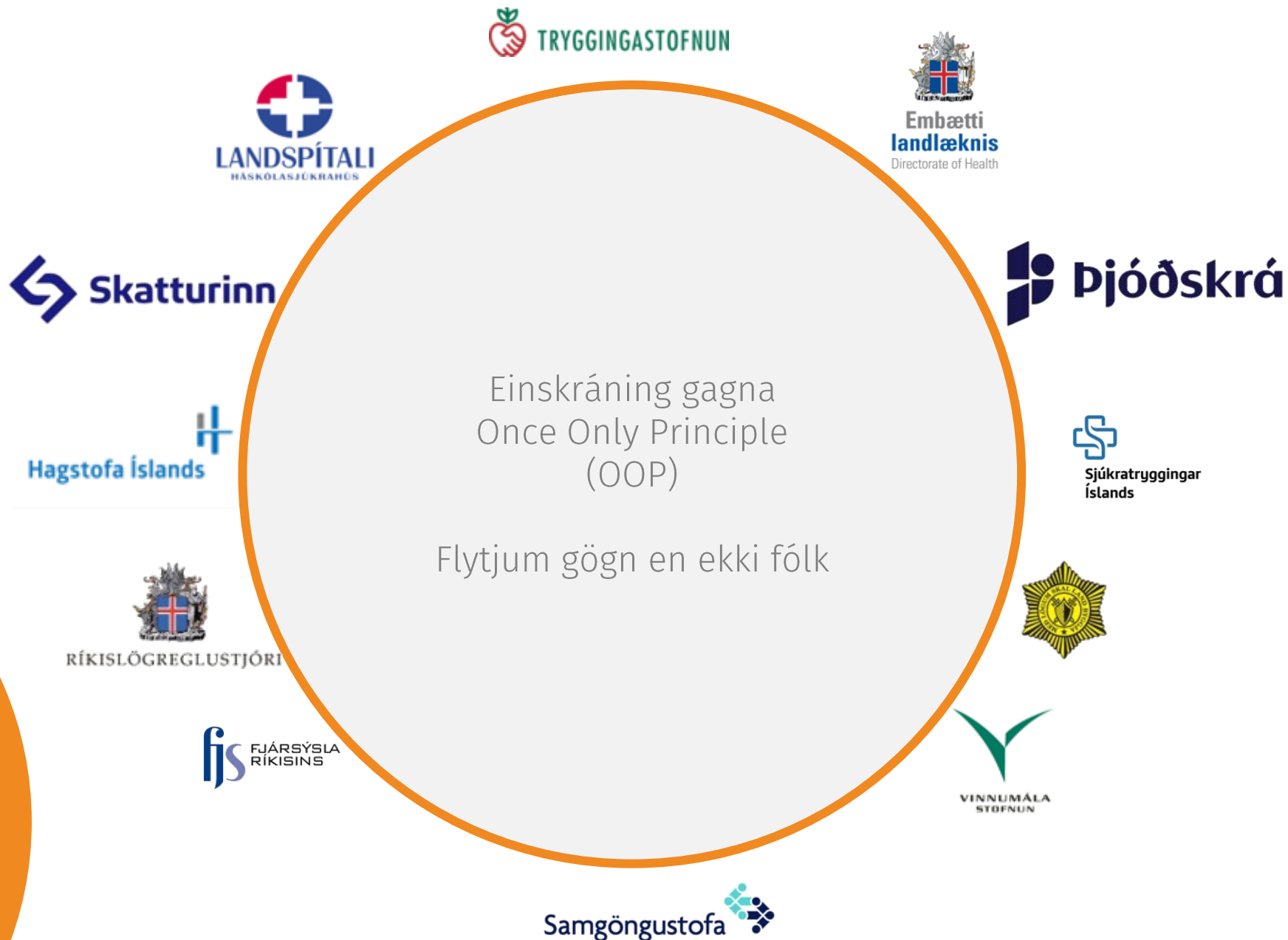




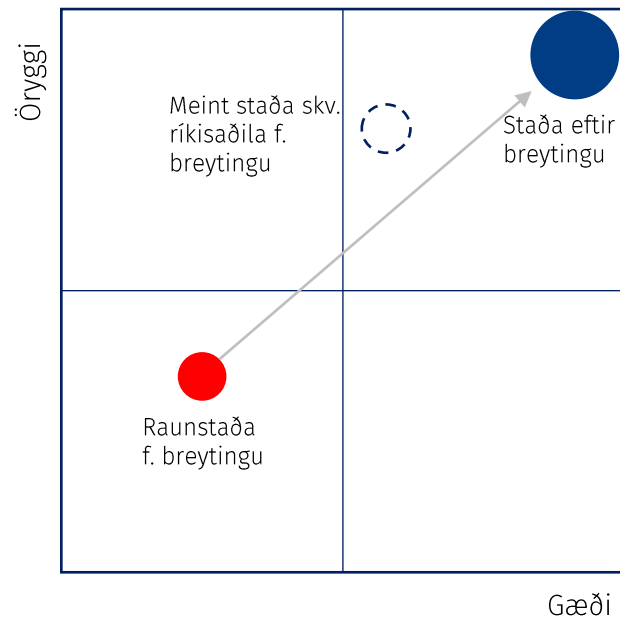


Aukin hag- og samnýting gagna er
forsenda margra þátta í ríkisrekstrinum

Betri ákvarðanir
Aukið virði
Betri þjónusta
Lægri kostnaður
Jákvæð umhverfisáhrif



Raunstaða oft ekki til samræmis við upplifun stjórnenda



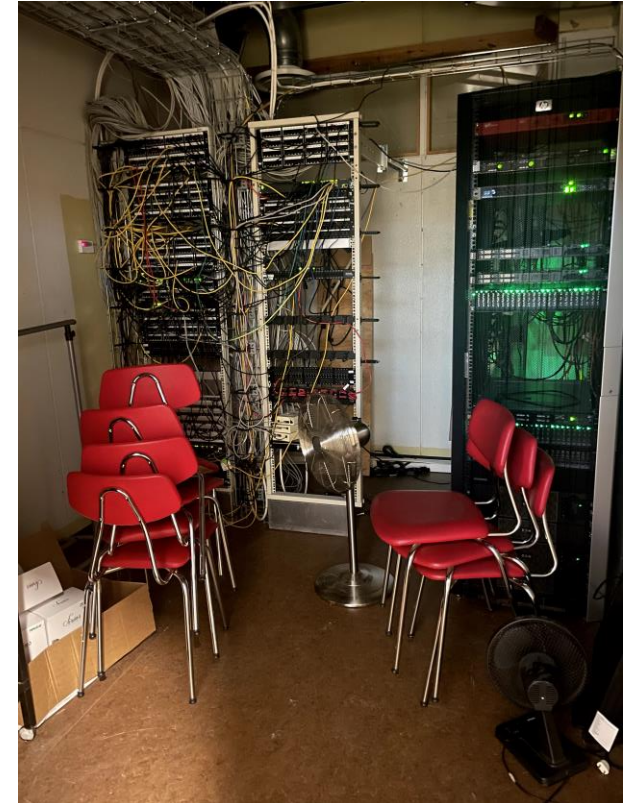
Ákvörðun um t.d. tæknilega högun eða val á upplýsingakerfi

Mótstaða við breytingu byggir gjarnan á því sjónarmiði að núverandi uppsetning sé betri en raunin er

Vélasalir eru víða hjá ríkisaðilum



Ímyndin af vélasal (hýsingu) hjá ríkisaðila



Raunveruleg staða hjá ríkisaðila

Dæmi

1

um meinta góða stöðu

„Gögn eru best geymd á eigin netþjónum í eigin húsnæði“

Algengt sjónarmið:

Stofnun er best til þess fallin að varðveita sín gögn í sem mestu öryggi og hefur til þess búnað og mannskap

Eigin netþjónar í eigin húsnæði er lausnin

Staðreynd:

Ríkisaðilar reka tugi vélasala

Veruleikinn:

Öryggi er betur háttað í hýsingarumhverfi skýjaþjónustu

Auðveldara að **brjótast inn** í kerfi „on prem“

Eigin netþjónar geta ekki þjónað sama **álagi** og í hýsingarumhverfi í skýjaþjónustu

Hýsingarumhverfi í skýi býður upp á mun meiri **sveigjanleika og fylgir tækniröfum** hverju sinni. Sam- og hagnýting **gagna** verður einnig auðveldari

Óhagræði í rekstri að reka eigin netþjóna

Einskráning gagna eykur öryggi og gæði þjónustu

Sömu gögnum er viðhaldið á mörgum stöðum í ríkiskerfinu með viðkomandi óhagræði og villuhættu

- Þjóðskrá
- Netföng
- Símanúmer
- Bankareikningur

Dæmi:

Ríkisaðili spyr þjónustuþega um netfang og bankareikning þegar ríkið býr nú þegar yfir upplýsingunum, t.d. hjá Skattinum

Dæmi

2

um meinta góða stöðu

Lekinn hjá Strætó afleiðing af lakri tæknilegri högun

Gagnalekinn hjá Strætó bs. var afleiðing af því að brotist var inn hjá fyrirtækinu. Strætó er einn þeirra aðila sem vistar **fullt afrit** af Þjóðskrá á eigin netþjón.

Núverandi fyrirkomulag verður því aldrei sterkara en veikasti hlekkurinn

Æskilegt fyrirkomulag:

Ein grunnskrá sem aðilar sækja í eftir þörfum

Grunnskráin sé vistuð með stöðluðum, alþjóðlegum hugbúnaði / gagnagrunni sem krefst ekki sérsmíði

Jákvæð þróun á viðhorfi stjórnenda til skýjalausna

Síðustu ár hefur umræða um skýjaþjónustur verið hávær. Tortryggni og skorður sem henni voru settar hjá ríkinu voru lengi vel í brennidepli.

Stjórnendur voru spurðir út í geymslu gagna í skýjaþjónustum. Sífellt fleiri stofnanir nýta sér nú skýið. Yfirgnæfandi meirihluti stjórnenda telur öruggt að vista gögn í skýjageymslum þar sem rúm 78% stjórnenda svöruðu þeirri spurningu játandi.

„Það er allt komið í skýið í dag sem gerði okkur kleift að aðlagast breyttu vinnuumhverfi vegna Covid“

stjórnandi meðal viðmælenda

78%

stjórnenda telja að öryggi gagna í skýi sé gott



Hvað má og hvað ekki?

Algengum fullyrðingum og spurningum svarað um rekstrar- og hýsingarumhverfi

DÆMI UM FULLYRÐINGAR SEM SVARAÐ ER

Öll kerfi ríkisaðila eiga að fara í skýið skv. skýjastefnunni

Gögn í skýjaþjónustu eru ekki örugg

Gögn verða óaðgengileg og tapast ef samband Íslands við umheiminn rofnar

Erlend stjórnvöld og eftirlitsstofnanir hafa aðgang að upplýsingum

Notkun stórra þjónustuaðila (Microsoft, Amazon, Google o.fl.) hamlar samkeppni og dregur úr nýsköpun

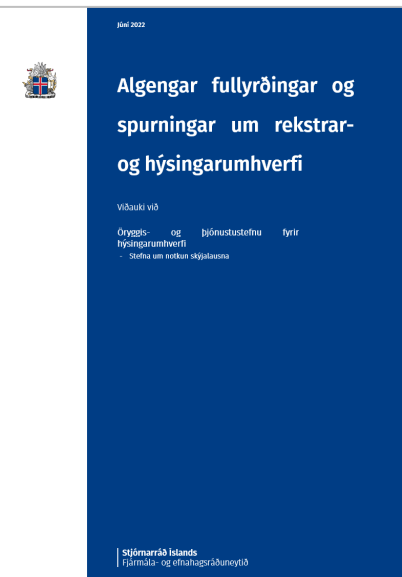
DÆMI UM SPURNINGAR SEM SVARAÐ ER

Mun ríkið geyma gögn sín í erlendum skýjaþjónustum og er það öruggt?

Bandarísk yfirvöld geta skv. lögum óskað eftir að fá gögn annarra þjóðríkja frá þjónustuaðilum svo fremi sem móðurfélag skýjaþjónustu hafi heimilisvist í Bandaríkjunum?

Ef Ísland verður sambandslaust við umheiminn er ótækt að gögnin liggi á erlendum netþjónum / Er gögnum íslenska ríkisins ekki best komið fyrir í innlendum gagnaverum?

Er löglegt að geyma gögn íslenska ríkisins utan Íslands?



Stuðningur af öryggisflokkun gagna

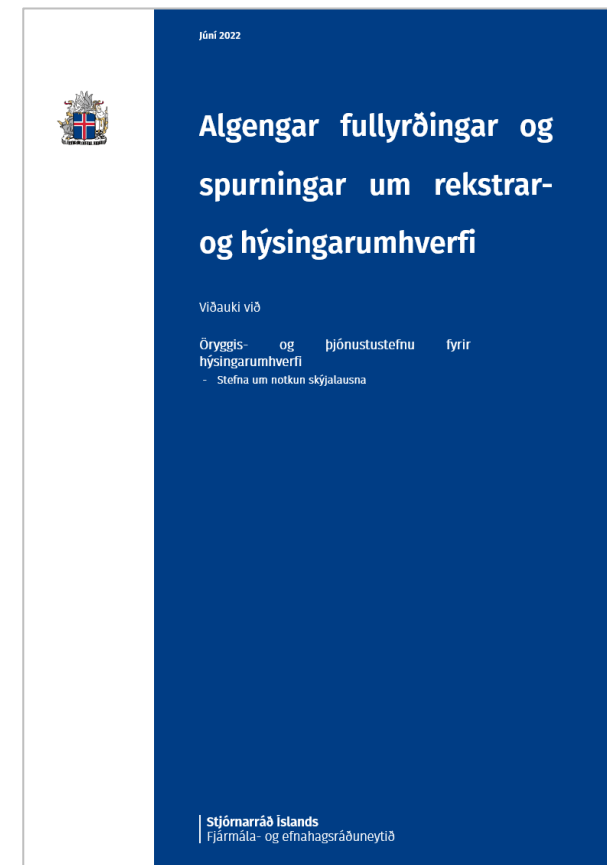
(e. Data Security Classification)



Samráðsferli lokið



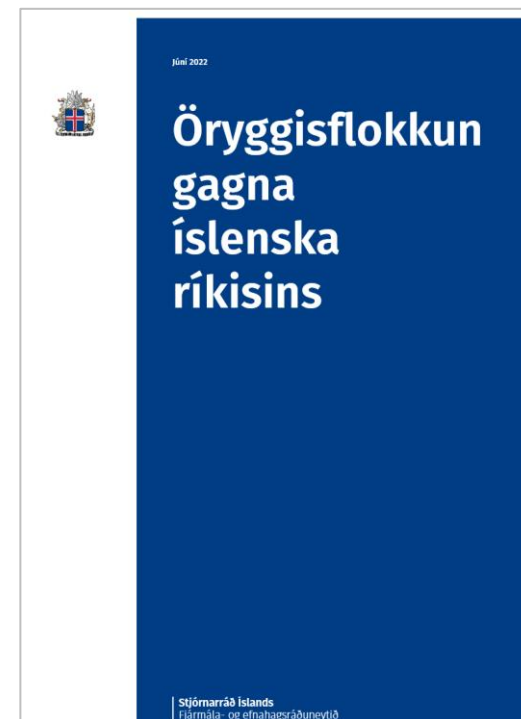
Birt



Viðauki við stefnu

Tilgangur öryggisflokkunar gagna

- Búa til samræmda öryggisflokkun fyrir öll gögn ríkisins og auka þannig skilvirkni í ákvörðunartöku um flokkun gagna
- Bæta kostnaðarmeðvitund sem fylgir hækkandi öryggisstigi
- Hámarka samnýtingu gagna – „Once only principle“
- Flytja gögn en ekki fólk



Öryggisflokkun þarf að vera aðgengileg

Einföld í notkun.

Allir nota sömu **grunnflokkun** til að einfalda og staðla samskipti og tryggja hámarksnýtingu og vernd gagna.

Gildir um **öll** gögn ríkisins, óháð formi gagnanna.

Nálgun á gögn út frá öryggi og hagnýtingu



Ákvarðanir um um öryggi og hagnýtingu séu teknar á meðvitaðan hátt út frá virði gagnanna



Ríki fara ólíkar leiðir í fjölda flokka

3

Secret

Sensitive

Official

4

Restricted

Confidential

Internal

Public

5

Top secret

Secret

Confidential

Sensitive

Unclassified

7

Restricted Data

Code Word classification

Top Secret

Secret

Confidential

Public Trust

Controlled Unclassified
Information (CUI)

Ástralía

Bandaríkin

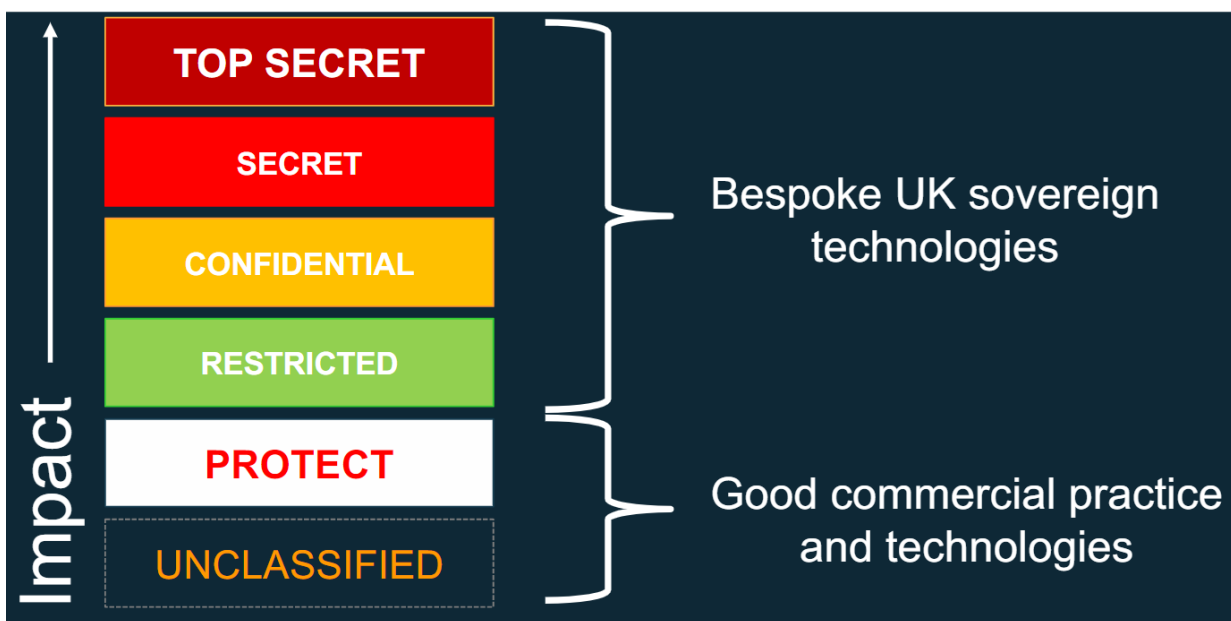
Bretland

Noregur

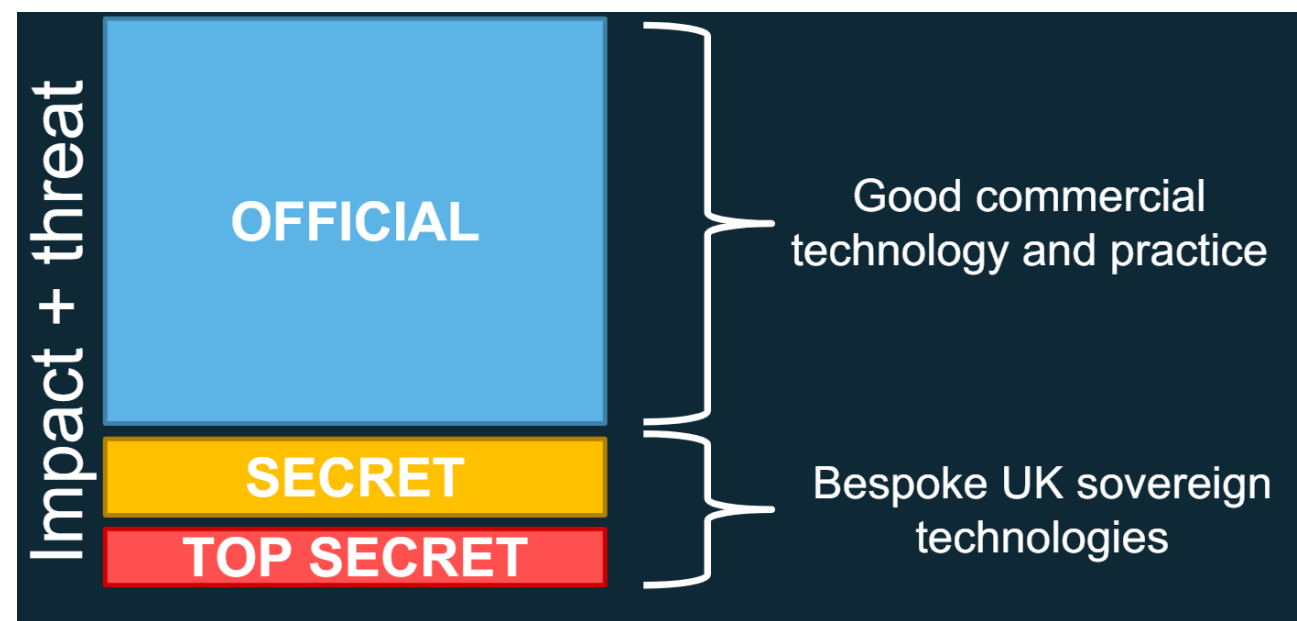
Finnland

Nýja-Sjáland

Öryggisflokkun í Bretlandi



PÁ



NÚ

Viðmið öryggisflokka íslenska ríkisins

e. Principles

1

Öll gögn hafa virði fyrir stjórnvald, einstakling, lögaðila eða samfélagið í heild.

2

Viðhafa þarf viðeigandi og gagnsæja meðferð og viðeigandi öryggisúrræði gagna byggt á virði þeirra og tilgangi.

3

Gögn skulu vera **opin og aðgengileg** öllum nema hagsmunir stjórnvalda, lögaðila, einstaklinga, almennings eða alþjóðasamstarf krefjist annars.

4

Aðgangsstýringar skulu byggja á **lágmarkun réttinda**, þ.e. aðeins þeir sem þurfa aðgang hafi hann.

5

Allir sem meðhöndla gögn í vörslu stjórnvalda, starfsfólk, þriðju aðilar og þjónustuaðilar skulu hafa **viðeigandi kunnáttu** í vörslu, umsýslu og öryggi gagna.

Öryggisflokkun

Byggir á **mikilvægi og virði** gagna og afleiðingum **óviðkomandi** aðgangs.

Tryggir **viðeigandi** öryggisstig, ekki of hátt og ekki of lágt.

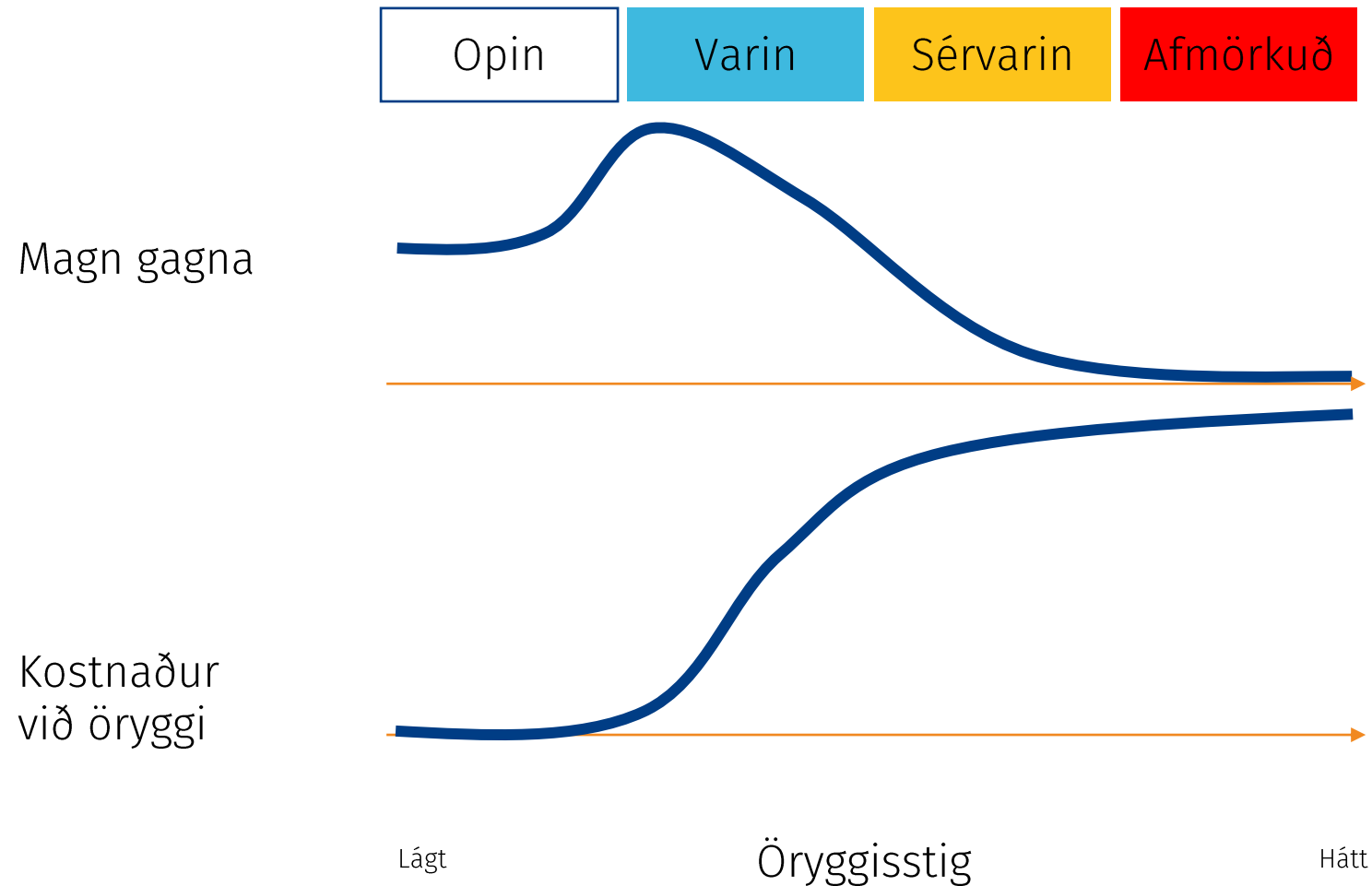
Krefst viðeigandi tæknilegra og skipulagslegra **varnaraðgerða** til að halda öryggisstigi.

Krefst kerfisbundins **áhættumats**.

Byggir á **trúnaði, réttleika, tiltækileika** (ISO 27001) auk **persónuverndar**.

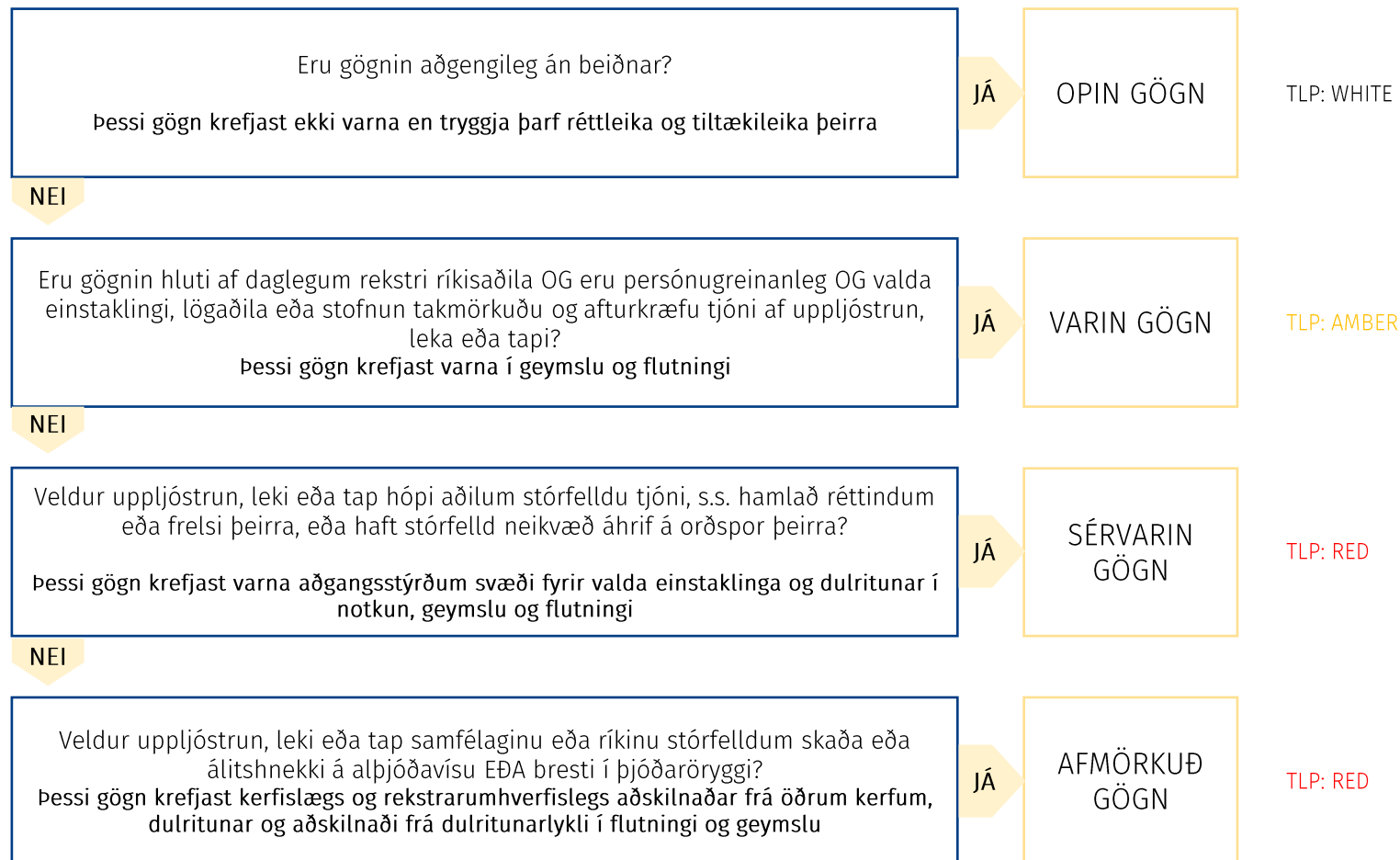
Tekur mið af hve miklu ytri aðili er tilbúinn til að **kosta til** að nálgast gögnin.

Fjórir öryggisflokkar gagna íslenska ríkisins



Skilgreiningar öryggisflokka ríkisins

Opin gögn	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.
Varin gögn	Öll gögn önnur en „opin gögn“ sem eru hluti af daglegum rekstri ríkisaðila.
Sérvarin gögn	Gögn sem vegna tímasetninga eða innihalds sem geta valdið víðtæku og langvarandi tjóni fyrir hópa einstaklinga, lögaðila eða ríkisaðila.
Afmörkuð gögn	Gögn sem eru viðkvæm fyrir samfélagið í heild eða stöðu þjóðarinnar á alþjóðavettvangi.





Dæmi um öryggisflokkun gagna

Má vista innan EES

Gagnasett	Ábyrgð / Varsla	Öryggisflokkur
Einstaklingsskrá (nafn, kt, lögheimili)	Þjóðskrá	Opin
Skráning viðkvæmra hella	UST	
Dómaúrskurðir (án persónuupplýsinga)	Dómsstólasýsla	
Fjárlög (birt)	FJR	
Fasteignamat og brunabótamat	Þjóðskrá	
Niðurstöður matvælaeftirlits sveitarfélags hjá veitingastöðum	MAST	Varin
Launaupplýsingar starfsfólks ríkisins	Fjársýsla ríkisins	
Sjúkraskrá einstaklings	Heilbrigðisstofnanir	
Sakaskrá einstaklings	Ríkissaksóknari	
Lyfjasaga einstaklings	Embætti landlæknis	
Skuldaskrá einstaklinga (allar skuldir einstaklinga yfir 300m)	HVIN	
Frumvörp (í vinnslu) - athugasemdir settar inn á vinnslustigi	Ráðuneyti	
Tölvupóstsamskipti ráðherra í ríkisstjórn	Stjórnarráðið	Sérvarin
Rannsókn lögreglu (mál sem er í vinnslu)	Ríkislögreglustjóri	
Innihald athugana (haldlögð gögn, vinnugögn) SKE	Samkeppniseftirlitið	
Fundargerðir ríkisstjórnar	FOR	Afmörkuð
Fundargögn Þjóðaröryggisráðs	FOR	
Vinnslugögn netöryggisráðs	HVIN	
Alþjóðasamningur ríkisins við NATO um gæslu í Miðjarðarhafinu	LHG	
Vinnugögn í undanfara afstöðu Íslands til kosninga í Öryggisráði SP	UTN	

Skal vista á Íslandi



Samráðsgátt

– opið samráð stjórnvalda við almenning



Samráð fyrirhugað
22.06.2022—19.08.2022



Til umsagnar
22.06.2022—19.08.2022



Niðurstöður í vinnslu frá
19.08.2022



Niðurstöður birtar

Öryggisflokkun gagna íslenska ríkisins

Mál nr. 103/2022 | Birt: 21.06.2022

Fjármála- og efnahagsráðuneytið | Annað

Málefnasvið: Hagskýrslugerð og grunnskrár

Niðurstöður í vinnslu

Umsagnarfrestur er liðinn (22.06.2022–19.08.2022). Umsagnir voru birtar jafnóðum og þær bárust. [Skoða umsagnir](#). Niðurstöður samráðsins verða birtar þegar unnið hefur verið úr þeim ábendingum og athugasemdum sem bárust.

Ábyrgðaraðili

Skrifstofa stjórnunar og umbóta
ainar.g.thoroddsen@fjr.is

Skjöl til samráðs

Öryggisflokkun gagna íslenska ríkisins

[Sækja skjal](#) - 606 kb



Takk fyrir

| **Stjórnarráð Íslands**
Fjármála- og efnahagsráðuneytið



BRIEFING ROOM

FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework

MARCH 25, 2022 • STATEMENTS AND RELEASES

The United States and the European Commission have committed to a new Trans-Atlantic Data Privacy Framework, which will foster trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union when it struck down in 2020 the Commission's adequacy decision underlying the EU-U.S. Privacy Shield framework.

This Framework will reestablish an important legal mechanism for transfers of EU personal data to the United States. The United States has committed to implement new safeguards to ensure that signals intelligence activities are necessary and proportionate in the pursuit of defined national security objectives, which will ensure the privacy of EU personal data and to create a new mechanism for EU individuals to seek redress if they believe they are unlawfully targeted by signals intelligence activities. This deal in principle reflects the strength of the enduring U.S.-EU relationship, as we continue to deepen our partnership based on our shared democratic values.