

Október 2022



# Öryggisflokkun gagna ríkisins - - Almenn kynning



# 1 Aðdragandi og tilefni vinnunnar

Bakgrunnur og forsaga verkefnisins

# 2 Hugmyndafræði og nálgun á öryggisflokka

Hvaða lykilforsendur liggja að baki öryggisflokkun gagna?

# 3 Öryggisflokkar gagna íslenska ríkisins



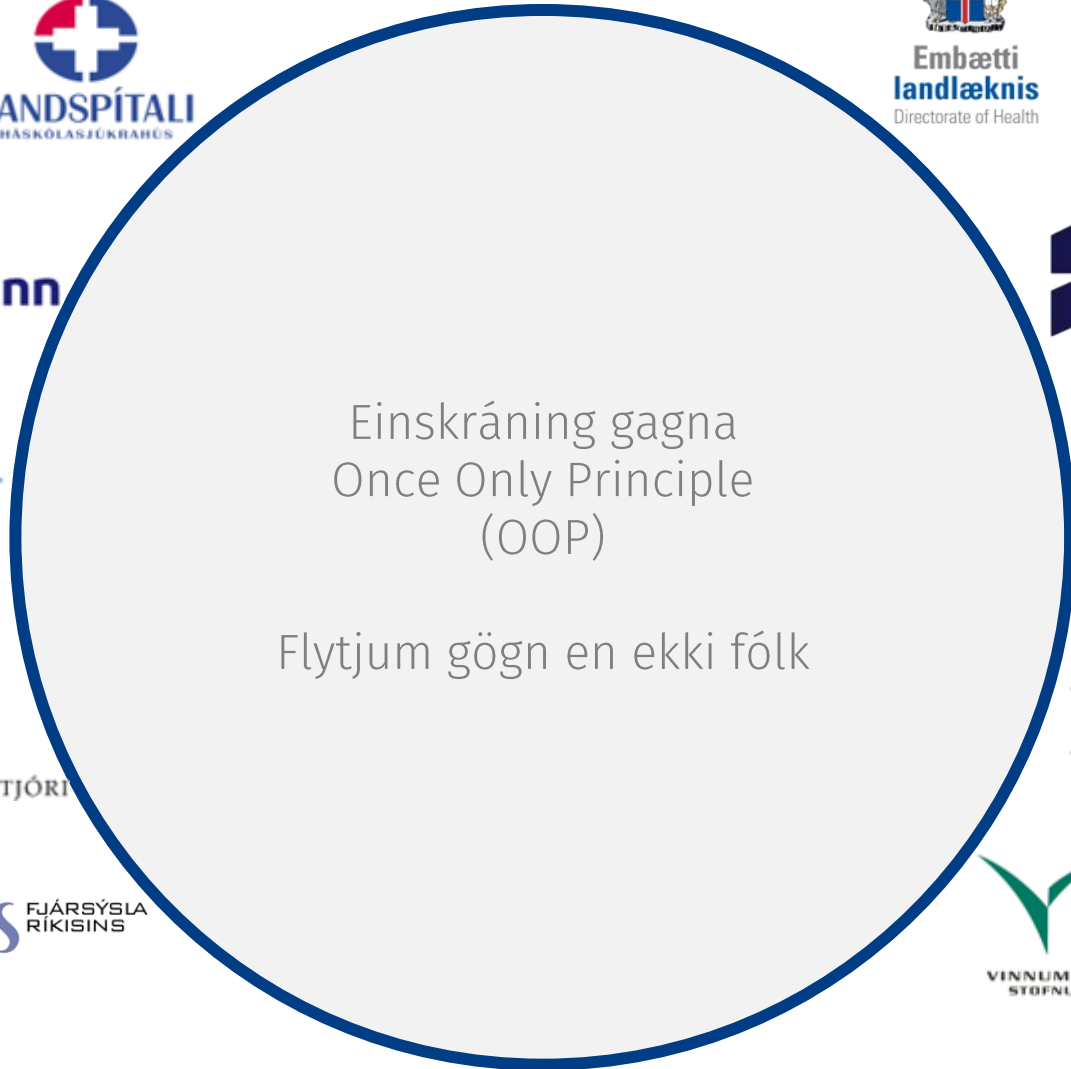
# Tilfni vinnu við öryggisflokkun gagna

- Meira öryggi gagna
- Meiri hagnýting gagna
- Betri þjónusta
- Betri ákvarðanir
- Hagkvæmari rekstur
- Skilvirkni og nútímavæðing innviða
- Aukið samræmi
- Upptaktur að nútímavæðingu laga
- Uppfylla alþjóðlegar skuldbindingar



# 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 – „Once only principle“
- Flytja gögn en ekki fólk
- Auðvelda flæði gagna vegna lífsviðburða



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

Betri ákvarðanir  
Aukið virði  
Betri þjónusta  
Lægri kostnaður  
Jákvæð umhverfisáhrif



# Vinnulag undirbúningshóps

Hópur með fulltrúum fjögurra ráðuneyta (FOR, FJR, DMR, HRN) og úr atvinnulífi

Fimm vinnufundir haldnir yfir 10 vikna tímabil frá desember 2021 til mars 2022

Horft til öryggisflokkana hjá öðrum þjóðríkjum

Samráðsferli

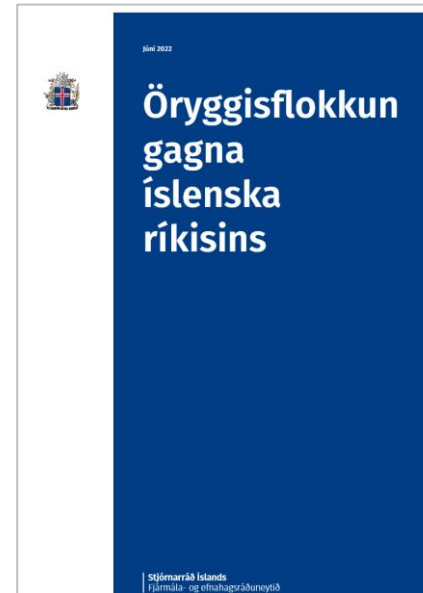
Birting



# Þróunin undirbyggir öruggara og betra rekstrarumhverfi



LOKIÐ



Lög um högun upplýsingatækni ríkisins

Lög / reglugerð sem eyðir óvissu um gögn og deilingu þeirra milli ríkisaðila

LOKIÐ



# Hvað má og hvað ekki?

Algengum fullyrðingum og spurningum svarað um rekstrar- og hýsingarumhverfi

## DÆMI UM FULLYRÐINGAR

Öll kerfi ríkisaðila eiga að fara í skjíð skv. skjástefnunni

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

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?

Júní 2022

## Algengar fullyrðingar og spurningar um rekstrar- og hýsingarumhverfi

Viðauki við

Öryggis- og þjónustustefna fyrir hýsingarumhverfi  
Stefna um notkun skýjalausa





# Tvær algengustu spurningarnar...

Má yfir höfuð vista gögn utan íslenskrar lögsögu?

Já, innan evrópska efnahagssvæðisins, nema mikilvægustu gögn þjóðarinnar sem varða þjóðaröryggi eða orðsperi landsins á alþjóðavettvangi, skv. Öryggisflokkum gagna ríkisins

Hvað gerist ef Ísland verður sambandslaust?

Sambandsleysi við útlönd er möguleiki en ólíklegur, ekki síst í ljósi fleiri tenginga við útlönd. Öryggisúrræðið er að vista afrit á Íslandi reglulega.

## 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. Sífelld 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





1

## Aðdragandi og tilefni vinnunnar

Bakgrunnur og forsaga verkefnisins

2

## Hugmyndafræði og nálgun á öryggisflokka

Hvaða lykilforsendur liggja að baki öryggisflokkun gagna

3

## Öryggisflokkar gagna íslenska ríkisins



# Öryggisflokkun þarf að vera aðgengileg

Einföld í notkun.

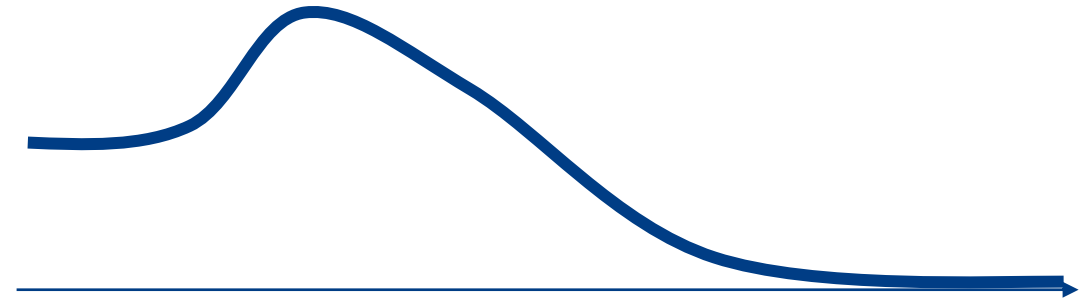
Allir nota sömu **grunnflokkun** til að einfalda og staðla samskipti og tryggja **hámarksnýtingu** og **vernd** gagna.

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

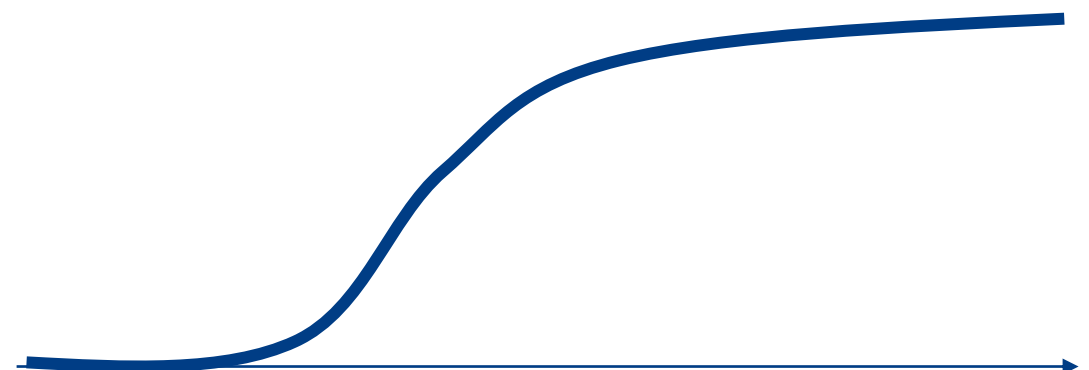


# Öryggisstig og kostnaður hanga saman

Magn gagna



Kostnaður við öryggi



Lágt

Öryggisstig

Hátt

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.

# Nálgun á gögn út frá öryggi og hagnýtingu



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



# Lykilbreytur í öryggisflokkun ríkisins

Réttindi og skyldur gagnvart einstaklingum og persónugreinanlegum upplýsingum.

Ógnir sem steðja að einstaklingum, stjórnvöldum eða samfélaginu vegna **uppljóstrunar, taps eða misnotkunar** upplýsinga.

Lögbundin **þjónusta** ríkisaðila.



# 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

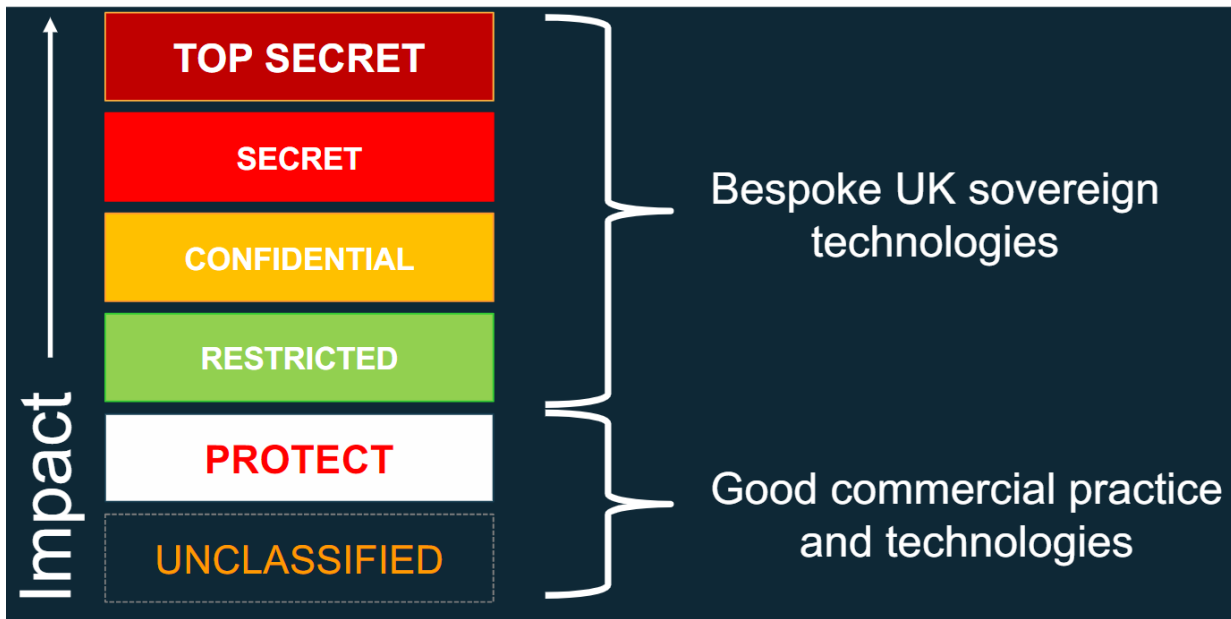
Finnland

Nýja-Sjáland

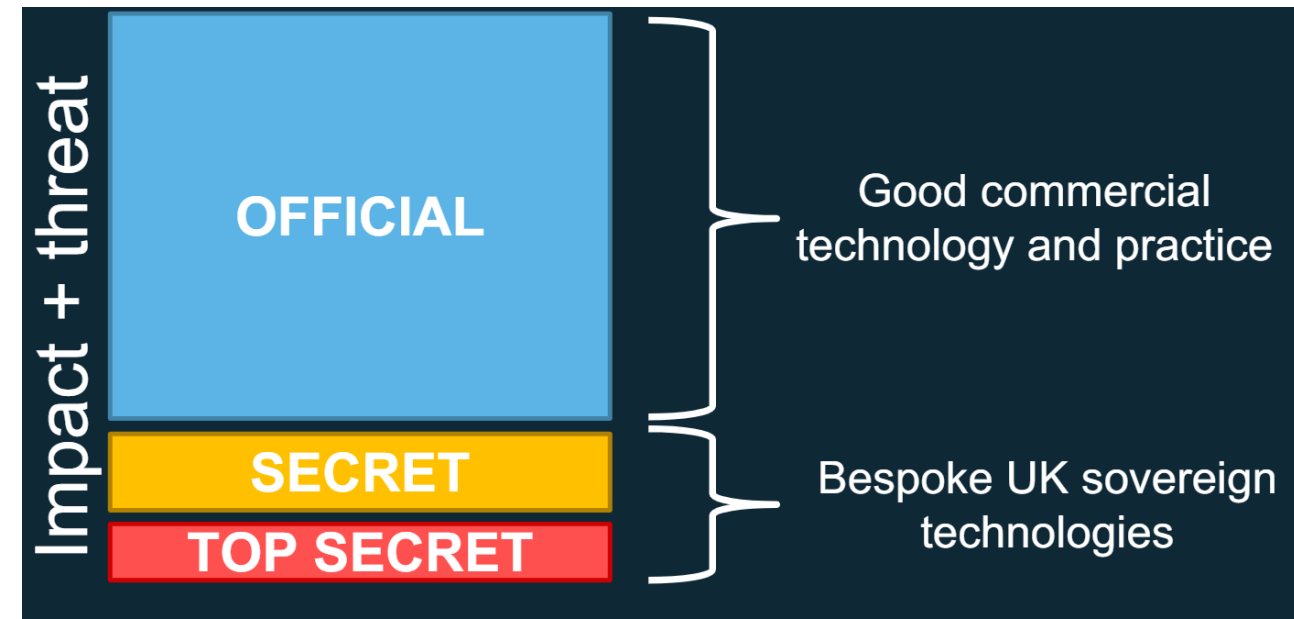




# Öryggisflokkun í Bretlandi



ÞÁ



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.



# Áherslur

1. Gögn skulu vera opin nema annað sé ákveðið
2. Öryggi gagna sé varið á viðeigandi hátt
3. Flokkun gagna skal vera kerfisbundin og samræmd
  1. Flokkar séu eins fáir og mögulegt er
  2. Flokkun sé nákvæm og í samræmi við aðstæður á hverjum tíma
  3. Flokkun byggji á virði gagna
4. Afleiðingar flokkunar skulu vera skýrar og skilgreindar
  1. Ábyrgð sé skýrt skilgreind
  2. Meðhöndlun gagna byggji á samræmdri flokkun



# Hlutverk og ábyrgð

**Ábyrgðaraðili\***: Sá aðili sem ber ábyrgð á skrá, tekur við gögnum og sem flokkar gögnin og ákveður meðhöndlun.

**Vörsluaðili**: Geta verið einn eða fleiri eða aðili innan sömu stofnunar og ábyrgðaraðili.

**Notandi**: Allir þeir sem hafa lögmætan aðgang að gögnunum.

\*Skilgreining á ábyrgðaraðila þarf ekki að fara saman með skilgreiningu ábyrgðaraðila í tengslum við lög um persónuvernd og vinnslu persónuupplýsinga 90/218



# 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.

# Afmörkun gagna í flokkun er mikilvæg

Flokkun í sem minnstum einingum til að varnir verði sem viðeigandi og flokkun skilvirk

Horfa til notkunar gagna þegar áhættur og afleiðingar eru metnar



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.



# Viðeigandi flokkun er líka mikilvæg

Of hátt öryggisstig getur valdið **gengisfellingu** öryggisflokka og minnkar gagnsæi.

Öryggisstig sem er umfram raunverulegar þarfir getur haldið **óhagræði**, auknum **kostnaði**, **hamlað** samnýtingu gagna og gert þjónustu stofnana **verri** fyrir almenning og samfélagið.

Huga þarf að öryggisstig tiltekinna gagna getur **hækkað** eða **lækkað** á mismunandi tímum.



1

Aðdragandi og tilefni vinnunnar

Bakgrunnur og forsaga verkefnisins

2

Hugmyndafræði og nálgun á öryggisflokka

Hvaða lykilforsendur liggja að baki öryggisflokkun gagna

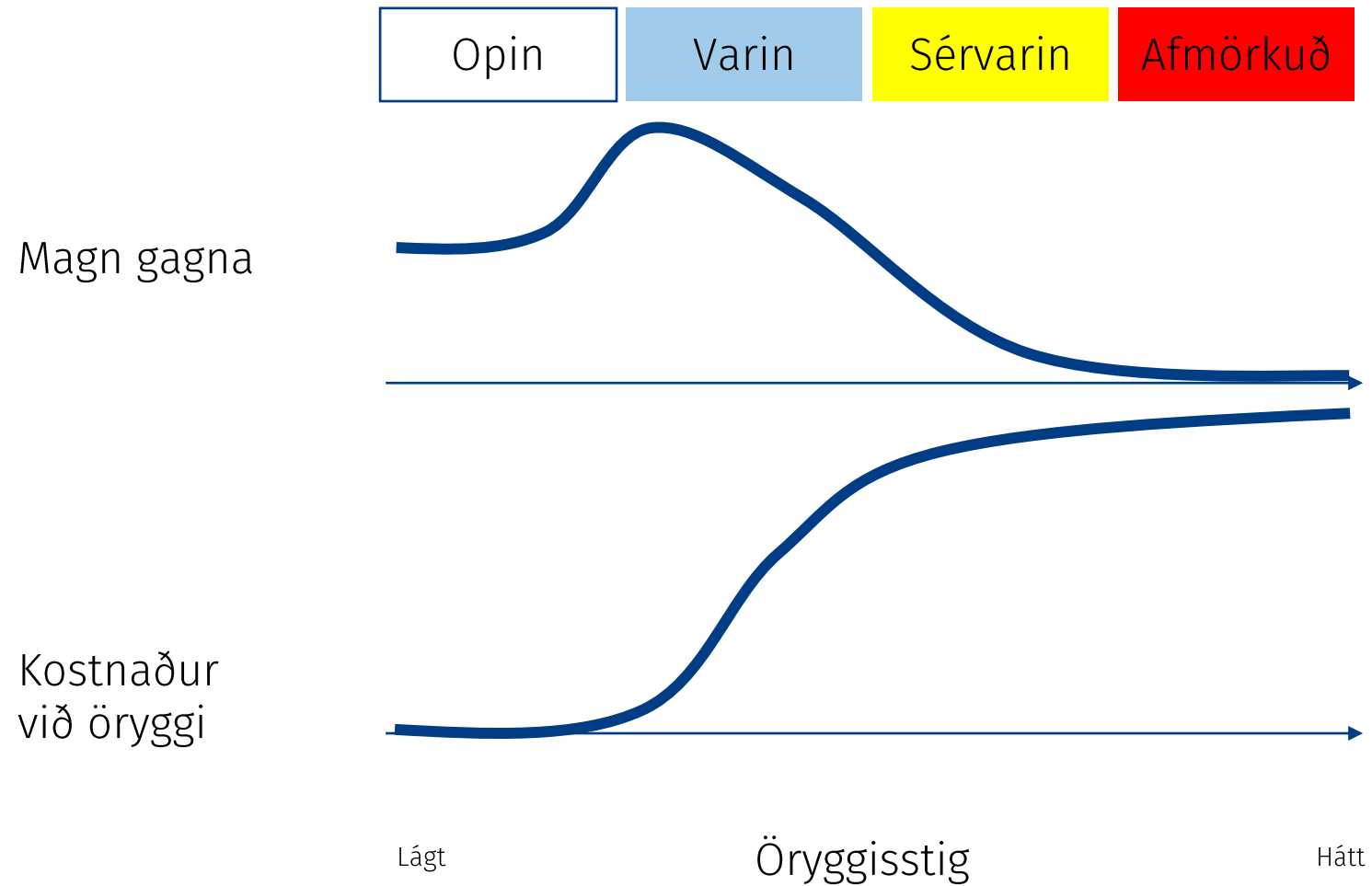
3

Öryggisflokkar gagna íslenska ríkisins





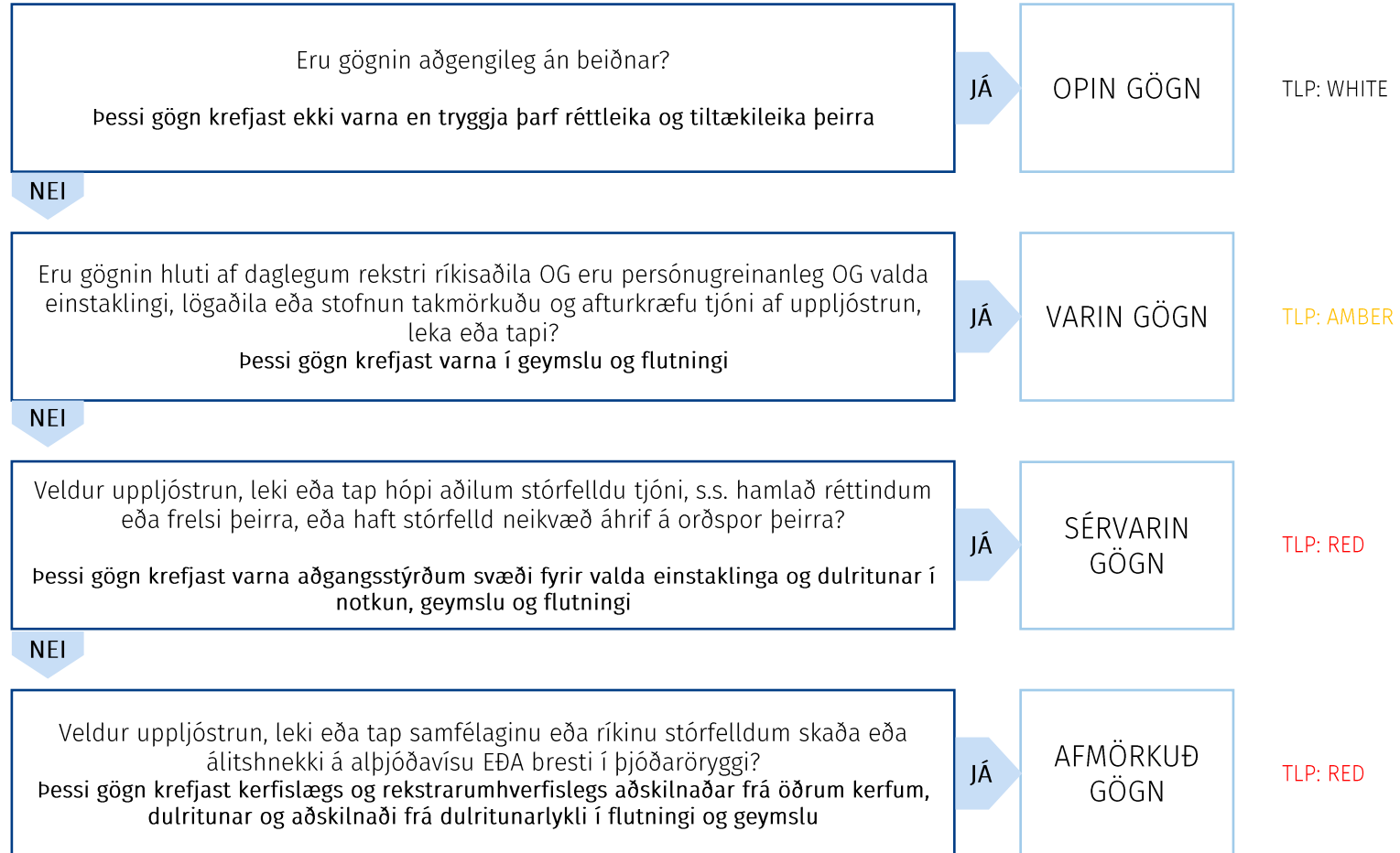
# Fjórir öryggisflokkar gagna íslenska ríkisins





# Skilgreiningar öryggisflokka ríkisins

Opin gögn	Ópersónugreinanleg gögn eða gögn sem eru <b>opin til notkunar og endurnotkunar</b> . 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 <b>daglegum rekstri</b> ríkisaðila
Sérvarin gögn	Gögn sem vegna tímasetninga eða innihalds sem geta valdið <b>viðtæku og langvarandi tjóni</b> fyrir hópa einstaklinga, lögaðila eða ríkisaðila.
Afmörkuð gögn	Gögn sem eru viðkvæm fyrir <b>samfélagið í heild</b> eða <b>stöðu þjóðarinnar</b> á alþjóðavettvangi.





# Öryggisflokkar á mannamáli

Öryggisflokkur	Lýsing	Ógn	Aðgangur	Hvaða reglur gilda?	Umfang
Ópin	Eru öllum aðgengileg en þarf að passa réttleika, aðgengi og gæði	Lítill	Allir	Ég má birta án takmarkana / sérstaks leyfis	
Varin	Eru aðgengileg þeim sem þurfa þau starfs sín vegna en krefjast stýringar (hópur / stofnun) til að verjast uppljóstrun	Lítill	Hópur	Ég má deila með hópi "innan starfssviðs"	
Sérvarin	Gögn sem krefjast upplýstrar ákvarðanatöku um dreifingu / aðgengi og aukinnar stýringar til að verjast uppljóstrun	Meðal	Notandi	Ég má deila með einstaklingi (e. need to know) vegna hlutverks síns	
Afmörkuð	Gögn sem vegna eðlis eða á lagagrundvelli er óheimilt að dreifa nema til tiltekinna aðila	Mikil	Notandi	Ég verð að spyrja eiganda um nákvæm fyrirmæli	



# Vistunarstaðir gagna

Flokkur	Staðsetning	Öryggisúrræði (viðmið)
Opin gögn	Hjá hæfum aðila* innan EES	Tryggja réttleika og tiltækileika.
Varin gögn	Hjá hæfum aðila* innan EES	Varin í flutningi yfir örugg samskiptakerfi með dulritun eða öðrum sambærilegum hætti. Auðkenning notenda. Atburðaskráning uppfletting og aðgangstilrauna.
Sérvarin gögn	Hjá hæfum aðila* innan EES	Dulritun (með eigin lykli) í geymslu og flutningi, sterk og margþátta auðkenning. Atburðaskráning uppflettinga og aðgangstilrauna.
Afmörkuð gögn	Á sértækum og aðskildum upplýsingakerfum í eigu viðkomandi ríkisaðila.	Allt ofangreint auk aðskilnaðar frá öðrum kerfum.

\* Hæfur aðili getur verið stofnunin sjálf eða samningsaðili, t.d. eftir innkaupaferli.



# Vistunarstaðir gagna - ráðstafanir

Áhætta	Staðsetning	Öryggisúrræði (viðmið)
Gögn verða ótiltæk ef erlent gagnasamband rofnar	Utan Íslands en innan EES	Hægt er að tryggja tiltækileika gagna og vinnslu með afritum gagna til Íslands.
Gögn eru haldlögð af erlendu stjórnvaldi	Erlendur aðili vistar gögn í gagnaveri innan EES	Samningar og ferlar hýsingaraðila sem taka á lögætum beiðnum yfirvalda þurfa að vera hluti af innkaupaferli þjónustunnar, óháð staðsetningu.
Aðgengi óviðkomandi starfsfólks þjónustuaðila að gögnum	Óháð staðsetningu	Öryggisferlar þjónustuaðila m.t.t. ráðninga og trúnaðar. Dulritun gagna (at-rest) með eigin lykli
Persónugreinanlegar upplýsingar fara til óöruggs lands	Óháð staðsetningu	Ábyrgðaraðili gerir nauðsynlegar kannanir á vinnsluaðilum óháð staðsetningu. Notkun nafnleyndar og lágmörkunar.



# Ákvörðunartré öryggisflokunar

	Opin	Varin	Sérvarin	Afmörkuð
<i>Persónuvernd:</i>				
Persónugreinanleg gögn (PII)	Nei	Já	Já	Já
<i>Afleiðingar uppljóstrunar:</i>				
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



# Afleiðingar af uppljóstrun, tapi og röngum upplýsingum

Flokkur	Opin	Varin	Sérvarin	Afmörkuð
<b>Skilgreining</b>	Ópersónugreinanleg gögn eða gögn sem eru opin til notkunar og endurnotkunar. Svo gögn teljist opin 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.
<b>Afleiðing uppljóstrunar</b>	Uppljóstrun hefur engin áhrif en villur/spilling gagna getur valdið óþægindum eða rangri ákvarðanatöku stjórnvalda eða annarra.	Uppljóstrun veldur stofnun eða tilteknum einstaklingi eða lögaðila óþægindum eða takmörkuðu fjárhagslegu eða orðsporstjóni sem mögulegt er að lágmarka. Uppljóstrun getur valdið stofnun eða öðrum aðila óhagræði í samningum eða viðræðum við ytri aðila.	Uppljóstrun gæti valdið samfélagshópum (einstaklingar og lögaðilar) eða stjórnvöldum fjárhagslegum eða ófenislegum verulegum skaða og haft áhrif á líf, frelsi eða réttindi einstaklinga.	Uppljóstrun stefnir öryggi og frelsi stórra samfélagshópa í verulega hættu.
		Uppljóstrun varðar við lög, t.d. brots á persónuvernd og kafla XIV í lögum nr. 19/1940.	Uppljóstrun getur stöðvað alla starfsemi viðkomandi stofnunar eða mikilvægra innviða.	Uppljóstrun skaðar samskipti við vinveittar þjóðir.
			Uppljóstrun hefur marktæk áhrif á fjármálastöðugleika.	Uppljóstrun varðar við lög um varnarmál (nr. 34/2008) þ.m.t. sektum eða fangelsi í allt að fimm ár.
<b>Afleiðing taps</b>	Lágmarksáhrif á ríkisaðila, gögn er hægt að endurskapa út frá öðrum gögnum án mikillar fyrirhafnar.	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.
	Ytri aðilar sem nýta gögn geta orðið fyrir óverulegu tjóni.			
<b>Afleiðing rangra uppl.</b>	Ríkisaðili verður fyrir lítillægum álitshnekkni 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 er að bæta. Fjárhagslegt tjón umfram getu eins ríkisaðila til að bæta.	Rangar upplýsingar gætu valdið alþjóðlegum deilum eða skaðað samskipti við vinveittar þjóðir.





# Sýnidæmi

## Grunnskrá

Margar af grunnskrám samfélagsins eru annars vegar mjög verðmætar m.t.t. varðveislu og viðhalds og svo mikil þörf fyrir að geta miðlað þeim hratt og örugga til ytri aðila.

Að uppfylla báðar kröfur í einu getur verið kostnaðarsamt eða ómögulegt. Því er nauðsynlegt að horfa til þessara tveggja notkunartilfella og sníða öryggisflokkun að hvoru tilfelli fyrir sig.

Miðlunareintak grunnskrár getur t.d. verið í dreifði þjónustu hjá einum eða fleiri skjáþjónustuaðilum meðan varðveislu eintak er aðeins aðgengilegt starfsfólki þess ríkisaðila sem ber ábyrgð á grunnskránni.

## Lækkaður flokkur

Gögn sem í upprunalegu formi geta verið varin eða sértækt er mögulegt að lækka niður um flokk. T.d. með að gera nöfnin ópersónugreinanleg með gervinöfnum eða samantektum,

Dæmi um slíkt geta verið heilbrigðisupplýsingar sem búið er að taka saman eða breyta til að gefa rannsakendum og öðrum aðilum mögulegt að nýta gögnin til vísindastarfs og nýsköpunar.

## Afmörkun gagna

Mörg gagnasöfn, þjónustur og hugbúnaðarkerfi innihalda í eðli sínu mjög ólík gögn. Greina þarf öryggisflokka út innhaldi kerfa en ekki kerfunum sjálfum svo offlokkun eigi sér ekki með auknu flækjustigi og útpynningu öryggisúrræða.

Tölvupóstkerfi ríkisaðila getur innihaldið gögn af ýmsu tagi. Huga þarf að tæknilegum og skipulagslegum úrræðum til að innleiða öryggisstýringar á tiltekna hluta tölvupósts en ekki útvíkka öryggisúrræði að óþörfu yfir gögn sem eru ekki af sama mikilvægisstigi, t.d. með dulritun á tiltekin samskipti, varðveislumerkingu eða öðrum hætti.

## UK Flokkun - dæmi

### OFFICIAL

The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

### SECRET

Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.

### TOP SECRET

HMG's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

3. Each classification provides for a baseline set of personnel, physical and information security controls that offer an appropriate level of protection against a typical threat profile. A top level controls framework is provided as an annex to this policy. As a minimum, all HMG information must be handled with care to comply with legal and regulatory obligations and reduce the risk of loss or inappropriate access. There is no requirement to mark routine OFFICIAL information.



# 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.